DEVELOPMENT OF INFORMATION TECHNOLOGY AND ITS IMPACT ON RIGHT TO PRIVACY – A CRITICAL STUDY

ABSTRACT

THESIS

SUBMITTED FOR THE AWARD OF THE DEGREE OF

Doctor of Philosophy

IN

LAW

BY

SANTOSH KUMAR

Under the supervision of

PROF. IQBAL ALI KHAN

(Chairman)

DEPARTMENT OF LAW

ALIGARH MUSLIM UNIVERSITY

ALIGARH (INDIA)

2010

The Information Technology, as we know it today, has a vast impact on storing information on every conceivable subject of interest to mankind which has transformed the communication system as whole. Advances in information technology and telecommunication networks have radically increased the amount of information and data that can be stored, retrieved, accessed and collated almost instantaneously. In real sense, the advancements in Information Technology have been very emphatic, but at the same time, these have negative and devastating impact also covering a wide range of issues of social concern.

In Indian perspective Information Technology related challenges is no longer an illusion but it indicates the prospective impact of the Information Communication Technology as the new frontiers of innovations in criminal activities covering the global perspective through the network of *world wide wave* (*www*) and other sophisticated and improved methods of technology.

In these technology oriented development, the most distinguished and intimate right of any human being is at stake which is better known as 'Right to Privacy'. The right to privacy refers to the specific right of an individual to control the collection, use and disclosure of personal information. Personal information could be in the form of personal records, habits and activities, family records, educational records, medical records, financial records and intimate communications such as telephonic talks and e-mail.

Further, Right to privacy is also affected in a manner that amounts to violation of public morality and decency in a civilized society with the use of convergence of technologies. The wider application of these innovative technologies has spawned a new and complex set of issues concerning individual privacy and information privacy i.e. data privacy.

The Constitution of India has not guaranteed the right to privacy as a fundamental right to the citizens but nevertheless the Supreme Court of India has come to the rescue of common citizens, time and again by construing "right to privacy" as a part of the "right to life and personal liberty". Although not to be recognized as a fundamental right, the right to privacy has gained Constitutional recognition in India.

The legal implications and standards of law to be observed in relation to protect the socio-cultural and moral norms seems to be inadequate in computer and communication related crimes. Therefore, it is high time to take it as a challenge and to develop the legal framework accordingly. The issue of information i.e. data privacy is also a prime concern to protect the system as well as society. Since, cyber security is a big challenge in current Indian perspective, thus we need a good legal framework in the area of cyber law, cyber security to protect e-transactions and the common interests of general public at large. In the present Indian legal context, the Information Technology Act, 2000 is a piece make legislation that is weak on the fronts of cyber security and other areas of cyber criminality and thus affecting the privacy rights of Indian citizens and other components of e-governance.

The innovations in communication technology and other way trends of development in Information Technology have gone into creating the fascinating innovations. To communicate with the help of Internet and *www* would not have had the impact that it has had in every sphere of life known to human civilization in prevailing scenario.

At a glance, the existing legal system and framework has shown inadequacy of legal protection dealing with Information Technology in relation to privacy rights. Moreover, the Constitution of India does not grant in any specific and express terms any right to privacy as such. Right to privacy is not enumerated as a Fundamental Right in the Constitution. However, such a right has been culled by the Supreme Court of India from

Article 21 and several other provisions of the Constitution read with the Directive Principles of State Policy.

Therefore, the present study is an attempt to bring together various perspectives of information technology and its manifold impact on 'Right to Privacy'. In this study, the Right to Privacy has been analyzed with theoretical, technological and socio-legal perspectives of information technology based system of telecommunication and electronic transaction in modern times.

The importance of the study is critical in order to evolve and to develop proper directional, controlled and systematic measures to protect the most cherished human want of privacy in well accepted and comprehensive manner.

The study has also been directed towards certain and limited glimpse of data protection legislations, conventions and directives covering the issues relating to data protection i.e. data privacy in comparative fashion prevailing in contemporary legal system of the world such as U.S.A., U.K. & European Union (EU) etc. in order to assess the contemporary challenges to law enforcement agencies and tech-based trans border means of communications.

1. The Choice of Topic

The following facts guided the choice:

I. The contemporary legal system is driven by the challenges of advances in science & technology.

II. The advent of Information technology and its applications have its own impact on human beings regarding the safety and security of their right of privacy.

III. The medium of information communication technology have to be regulated and controlled by developing up-to-date legal mechanisms in present system of global networks of communication such as

Internet and world wide networks of communication technology.

IV. Indian legal system lacking behind to control the growing menace of cyber based criminality.

V. A viable and effective mechanism is required to control the system with efficient and effective legal frame work.

2. Need for the Study

The need for the present research originates from debatable issue of right to privacy in contemporary development of modern versions of science and technology. This study may fulfill the need and may also provide some valuable contributions to develop the technology based legal system for the benefit of modern civilized society in order to meet out the global perspectives of legal developments. The concern of individual privacy and information privacy i.e. data privacy has urgent need for research in this challenging area.

3. The Objective of the Study

The objective is to undertake the present research work:

I. To analyze the development of information technology and its impact on right to privacy.

II. To examine the current and existing legal frame work to protect the right to privacy.

III. To give effect the emphasis on protection of information relating to privacy in this age of Internet and well advanced system of telecommunication.

IV. To develop the new mechanism of regulation and control such as establishment of 'Cyber Regulatory Authority of India' (CRAI) and widening the present ambit of information technology related legislations.

V. To emphasize the advancements and changes in existing cyber

practices of regulation and enforcement.

VI. To make cyber legislation more stringent and effective by the making of special laws and constitutional amendments.

VIII. To add and empower the enforcement agencies with proper development of techno-legal courses and personnel such as introduction of models of cyber policing system based on global pattern and high standards of competence.

4. Research Hypothesis

The present research proceeds on the following hypothesis:

I. Development of information Technology has serious impact on 'Right to Privacy' and the extent is unlimited with constant development of science and technology.

II. The innovation and application of information technology is a developmental process, therefore the legal frame work should also be developed at required pace.

III. The constitutional provisions and judicial responses in relation to breach of privacy and confidentiality are not so explicit to resolve the malady.

IV. At present the Information Communication Technology (ICT) is a very topical issue not only in India but in the rest of the countries. To meet out the resulting challenges legal mechanisms are to be evolved, developed and proper restrictions to safeguard the individual interest as well as national Interest must be taken.

V. Impact of techno-legal advancement and contemporary requirement of regulation and control of data privacy.

5. Scope and Limitations of the study

The scope is restricted to the following:

I. Technological development and information privacy under the legal framework.

II. Restrictions on information super highways with due importance to information privacy and data privacy i.e. dissemination of personal data.

III. Unlimited possibilities of Internet & *www* and restricted use of data by application of data protection laws.

IV. Regulation and control of information technology to protect the right to privacy.

V. Indian legal framework and control mechanisms of confidentiality and privacy.

VI. Legal limitations and technological implications, difficulties and possible remedial measures.

6. Impact of the study

The technology has always been the boon or bane to human civilizations and in strict sense to human beings. The subject matter of study is so delicate that it has its own inherent controversies and concerns. Therefore, the impact of the study would certainly helpful to add and to develop the existing legal framework on the subject. However, the adoption of the information technology i.e. Internet and *www* would not have had the impact that it had as so such brain power has involved into creating the problem of abuse or misuse of this fascinating innovation of Information Technology.

7. Research Methodology

The study is doctrinal and analytical. It is based on comparative and critical study of Constitutional and legal mechanisms in international legal systems particularly U.S.A., U.K. and European Union (EU) and Indian Legal framework relating to information technology. The study has its own limitation due to the impact of constant developing technologies and its applications in this high-tech system of governance and legal developments.

8. Chapter-wise Introduction

The brief *chapter-wise* contents are, as under:

Chapter-1 pertains to a brief retrospect of Computer and Internet related developments and a summary of Information Technology related legal infrastructure based on *UNCITRAL* model law on electronic commerce in Indian legal framework known as Information Technology Act, 2000.

Chapter-2 deals with techno-legal developments in relation to its impact on right to privacy. The critical study has been included based on the constitutional perspective and case-by-case development as per Indian Judicial response and foreign cases.

Chapter-3 attempts to reflect the issue of Information Privacy (i.e. data privacy) and impact of technology on it. Since, the convergence of technology has special relevance with respect to technology based activities on the Internet thus its consequences in electronic format on data privacy has been highlighted.

Chapter-4 deals with the aspects relating to right to privacy and critical issue of data protection in Indian legal perspective. A brief analysis of relevant provisions of Information Technology Act, 2000 has been incorporated to reflect the current Indian Legal position.

Chapter-5 attempts to give the legal position of right to privacy and data privacy related legislations in various countries of the world such as U.S.A., U.K., The council of Europe, Japan and European Union etc. to provide a concept of data protection and other related issues of trans border flow of information.

Chapter-6 deals with remedial perspectives of individual privacy and data privacy in order to develop a model law on data protection in relation to the current needs of privacy protection.

Suggestions

The following suggestions are advanced by the researcher to strengthen the legal infrastructure relating to Information Technology and its impact on several dimensions of privacy:

(1) The Indian Constitution does not guarantee the Right to Privacy as a fundamental right. The sole credit goes to the Indian judiciary for recognizing the concept of privacy because neither the Constitution nor any other statute has defined the concept. Still a lot more has to be done for the recognition and protection of privacy by law in India. As a matter of fact this concept is in primitive stage of its development but its development is bound to have tremendous effect on the individual's living with the development of Information Technology. Therefore, it is suggested that the 'Right to Privacy' should be recognized as a separate Fundamental Right with comprehensive guidelines on this sensitive issue of the privacy.

(2) The fundamental right of freedom of speech and expression as enshrined in the Constitution of India extends to the medium of Information Communication Technology as well and therefore every citizen has a freedom to acquire or share knowledge (or information) using Information Technology and related sources, subject only to reasonable restrictions. Since, imposing "reasonable restrictions" on the Information Communication Technology has certain limitations; therefore a legal framework based on the principle of 'reasonableness and due care' has to be adopted. For this purpose, the Information Technology Act, 2000 may be amended and enlarged to equate it with the concept of "balanced flow of information".

(3) The right of an individual to protect his personal information is a basic civil right, and is recognized as such the world over. Thus in relation to data and individual privacy, India should enact legislation

to protect the personal data of individuals, and to ensure that data collected for a particular purpose is used for that specific purpose only.

(4) Governments and other empowered authorities are interested in what passes over on the Internet and are making efforts to devise various means of exercising a substantive degree of control by way of interception in relation to information communication technologies, as a consequence the organizations and individuals using these techniques are concerned with their privacy and security of data. These genuine concerns can be meted out by wide application of encryption methods to control the privacy of data and theft of valuable information.

(5) Earlier, before the enactment of Information Technology Act, 2000, no legal infrastructure was available in Indian legal context, which explicitly recognized or denied the general principle that information, records in electronic form should be given legal effect.

Since, the Information Technology Act, 2000, intended to deal with computer abuse and e-commerce matters, contains brief mentions of data protection issues but does not lay down specific privacy principles.

Yet the making of Information Technology Act, 2000 was a landmark in Indian legislative history to combat with emerging and developing technological threats, but in this era of diagonal changes in technology the frictional changes in law is also required to resolve the maladies.

(6) The present Information Technology (IT) Act is soft when it comes to curb cyber criminality, thus there is need for more deterrence in the IT Act. Cyber crimes have to be dealt with very strongly because this is being done by knowledgeable people and to deal with it the need of

the hour is for training the investigating, prosecuting and judicial agencies to respond to the challenges posed by cyber criminals.

(7) The balance must be struck in relation to the extent of legislative provisions and variations by agreement in regular format of paper based transactions, that flexibility should be maintained in information technology based transactions i.e. electronic transactions. This should be subject to fairness and reasonableness test as applicable in common legal parlance.

(8) The law in India includes a number of different provisions, which requires a document to be in writing. In a number of cases, it is unlikely that an electronic form of document would satisfy these requirements. It is imperative that a data message should satisfy any of these requirements for information to be in writing. This may be developed on functional equivalence to the United Nations Commission on International Trade Law ('*UNCITRAL*') working group on Electronic Commerce completed work on its model law on Electronic Commerce in 1996, and its draft on international legislation on information security.

(9) The controlling and regulating authorities have the immense duty to evolve, develop and to up-date the rules and practices which recognize the new computer based technology for the effective implementation of e-governance and at the same time to protect the national as well as public interest.

(10) An information infrastructure already exists, but it is not integrated as whole. Telephones, radio, transistors, televisions, computers and fax machines are used everyday to receive, store, Process, perform, display and to transmit data, text, voice, sound and images in offices, homes as well as in business within the country and outside the country. The above mentioned separate communication networks

required an integration of legal control and regulation framework as digital code.

(11) The Indian communication system is still governed by the more than hundred years old law legislations mainly the Indian Telegraph Act, 1885 and supported by the Indian Wireless Act, 1933. Considering the substantial technological developments and changes these laws must be replaced by new legislations giving effect to emerging scenario of digital technology.

(12) As per agency to regulate telecom sector i.e. 'Telecom Regulatory Authority of India' (TRAI) was established in 1997, the regulator for cyberspace may also be made possible with proposed name as 'Cyber Regulatory Authority of India' (CRAI), to control and regulate the activities on cyberspace.

In the present Indian scenario the efficiency and effectiveness in the implementation of cyber regulations and control measures requires structural changes in the framework as well as strengthening the e-court infrastructure and their capabilities to deliver the speedy justice. The public education regarding the use of cyberspace is immensely needed to educate and aware the general public in relation to cyber based criminality and related developments.

In view of inherent technical difficulties and radical changes in application of technology, it is high time to rethink cyber laws to provide protection to users by developing the techno-legal framework in order to optimize more creative side or benefits of information communication technologies.

In short, every one should be aware of and actively involve in preventing and solving together the destructive side of information communication technology with an appropriate balance between regulations and self regulations subject to the different types of activities in cyberspace.

To keep up with the pace of technological innovations laws should be rethought with the impact of Internet in mind to ensure the integrity of cherished human values of privacy.

Last but not the least, the law must be synchronized and developed with all possibilities to sustain the good moral and ethical values in order to overcome the challenges posed by technological advancements. The uniformity in law and universal codification of Internet law must be evolved by the world community to protect the privacy and confidentiality in this database driven age.

DEVELOPMENT OF INFORMATION TECHNOLOGY AND ITS IMPACT ON RIGHT TO PRIVACY – A CRITICAL STUDY

THESIS

SUBMITTED FOR THE AWARD OF THE DEGREE OF

Doctor of Philosophy

IN

LAW

BY

SANTOSH KUMAR

Under the supervision of

PROF. IQBAL ALI KHAN
(Chairman)

DEPARTMENT OF LAW
ALIGARH MUSLIM UNIVERSITY
ALIGARH (INDIA)

2010

Dedicated

to

My Family

PROF. IQBAL ALI KHAN
Chairman

DEPARTMENT OF LAW
ALIGARH MUSLIM UNIVERSITY
ALIGARH (U.P.) (INDIA)

Dated:.....

Certificate

It gives me immense pleasure to certify that **Mr. Santosh Kumar**, Research Scholar, Department of Law, AMU, Aligarh has completed his Ph.D. thesis, entitled ***"DEVELOPMENT OF INFORMATION TECHNOLOGY AND ITS IMPACT ON RIGHT TO PRIVACY-A CRITICAL STUDY"*** under my supervision. The material incorporated in the thesis has been collected from various sources; he has used and analyzed aforesaid material systematically. The present work is an original contribution in the field of Information Technology Law.

14-7-10

PROF. IQBAL ALI KHAN

ACKNOWLEDGEMENT

All Glory to the God without whose blessings this work would not have been possible. I pray to God for blessings and success.

I wish to express my most humble, sincere and profound gratitude to my erudite supervisor ***Prof. Iqbal Ali Khan*** *(Chairman), Department of Law, AMU, Aligarh for his cognate attitude, academic excellence, skillful guidance, continued encouragements towards this work, his keen interest and immense help in an indefatigable and perspicacious manner emphatically paved the way for me to complete the study.*

I owe a deep sense of gratitude to my esteemed teacher Prof. Mohd. Shabbir (Dean), Faculty of Law, AMU, Aligarh, for his academic guidance and valuable support.

I feel immense pleasure to record my sincere thanks to my esteemed teachers Prof. Saleem Akhtar, Prof. Akhlaq Ahmed, Dr. Zaheeruddin, Dr. Javed Talib, Dr. Zubair A. Khan, Dr.Shakeel Samadani, Dr.Badar Ahmed, Dr.Shakeel Ahmed, Dr.Z.M.Nomani, Dr. Zafar Eqbal and for their care and encouragement.

I am equally beholden to my learned teachers Prof. Faizan Mustafa,Dr. Mohd.Ashraf, Dr. M.Waseem Ali, Dr. Hashmat Ali Khan for their inspiration and generous consideration.

My immense thanks to Prof. R.S.Varshney (Retd.) for his

guidance, gentle criticism and continued encouragement.

I feel immense pleasure in acknowledging my friends Dr. H.R.Khan (PCSJ,UP), Prof.Shamsul Haq, Dr. Mayur Vikram Chandra (Advocate, Supreme Court), Dr. Gaurav Kaushik, Mr. Lalit Mohan Sharma (Company Secretary), Dr. Masud, Dr. Haider, Mr. Jetendra Singh(Advocate, Supreme Court of India), Mr.Yogendra Singh and Mr.Ashok Agarwal(Advocate) for their care, inspirational backup and support.

My thanks also to all my classmates Dr.Nagma Azhar, Dr. Urusa, Dr. Mohd. Khalid and Mr. Qazi M.Usman for their inspiration and support.

I must express my sincere gratitude and indebtedness to all the members of my family for their nice support and patience. I must express my deep sense of regard to my father Shri R.K.Mishra for his affectionate encouragement and blessings throughout my academic life. Special mention requires for my younger sisters Poonam and Roopam for their care and nice support.

The care displayed by my wife Dr. Suman Tiwari along with my daughter Ananya deserves special mention in my scheme of thank, it is her loveable support which enabled me to accomplish this task.

My thanks are also due to my father in law Prof.R.P.Tiwari, Head, Deptt. of Sanskrit, H.N.B.Garhwal University,Srinagar(Garhwal) for inspiration and all along support.

Last, but not the least my thanks to whole ministerial staff and library staff, Faculty of Law, AMU for their cooperation at each and every stage in the completion of the study.

My special thanks to Mr. Mohd.Sharif Khan, Mr.Yasin and Mr. Azeem for their valuable support.

My immense thanks to Mr. Aftab Ahmad 'Classic Computers' for the nice typesetting of the thesis.

My immense thanks to 'Diamond Book Binding Works' for the nice binding works of thesis.

My immense thanks also to all my other well-wishers whose names are not mentioned here by chance.

(Santosh Kumar)

CONTENTS

ABBREVIATIONS

AIR	All India Reporter
Art	Article
DB	Division Bench
Dept.	Department
Ed	Editor
Edn	Edition
Etc.	Etcetera
Ibid	In the same place
i.e.	That is
OECD	Organization for Economic Co-operation and Development
P.	Page
SCC	Supreme Court Cases
IT	Information Technology
UN	United Nations
UDHR	Universal Declaration of Human Rights
EU	European Union
USA	United States of America
UK	United Kingdom
VOL.	Volume
V.	Versus
ICT	Information Communication Technology
TRAI	Telecom Regulatory Authority of India

UNCITRAL	United Nations Commission on International Trade Law
WWW.	World Wide Wave
FTP	File Transfer Protocol
ICCC	International Computer Communications Conference
HTML	Hyper Text Mark Up Language
HTTP	Hyper Text Transfer Protocol
URL	Universal Resource Locator
ISP	Internet Service Provider
PIL	Public Interest Litigation
DPSP	Directive Principles of State Policy
FR	Fundamental Right
ICR	Information Communication Revolution
e-commerce	Electronic Commerce
e-transaction	Electronic Transaction
e-governance	Electronic Governance
PC	Personal Computer
DDOS	Distributive Denial of Service
e-mail	Electronic Mail
GIF	Graphic Interchange Format
IP	Internet Protocol
TTPs	Trusted Third Parties
e-Crime	Electronic Crime
USML	US Munitions List

ICCPR	**International Covenant on Civil and Political Rights**
ICCP	**Information Computers and Communication Policy**
ECHR	**European Convention on Human Rights**
UNGA	**United Nations General Assembly**
FTC	**Federal Trade Commission**
EEA	**European Economic Area**

LIST OF CASES

- Raja v. P.Srinivasan AIR 2010 Madras 77 (DB)
- Albert v. Strange, (1849) 1 Mac&G25:41ER1171
- America online Inc. v. LCGM, Inc., F.supp 2d 444
- American Civil Liberties Union v. RENO, 929 F. Supp.824 (1996)
- K. Parthsarathy v. State of Andhra Pradesh, AIR 2000 AP 156
- Bowers v. Hardwick, 478 US 186(1986)
- Compu Serve v. Cyber Promotion,1962 F.supp.1015
- Cyber Promotions, Inc. v. America Online, 948F.supp.436
- Daniel Bernstein v. United States (Dept. of State), 922 F. Supp. 1426 (N. D. Cal.1996)
- Data Protection Registrar v. Francis Joseph Griffin (QB, 22 February 1993)
- District Registrar and Collector v. Canara Bank, (2005) 1 SCC 496
- Eisenstadt v. Baird, [1972] 405 U S 438
- Equifax Europe Ltd v. Data Protection Registrar (1991), Case DA/90 25/49/7

- FTC v. Toysmart.Com, LLC, and Toysmart.Com, Inc, Case no.00-13995-CJK, 2000
- Gaskin v. United Kingdom, (1989) 12 EHRR 36
- Govind v. State of Madhya Pradesh, AIR 1975 SC 1378
- Griswold v. Connecticut, (1965) 381 US 479
- Innovation (Mail Order) Ltd v. Data Protection Registrar, (29 Sept. 1993; Case DA/92 31/49/1)
- Intel Corporation v. Kourosh Kenneth Hamidi, 30 cal rptr.4th 1342
- Jane Roe v. Henry Wade, 410US 113(1973)
- Katz v. US, 389 US 347 (1967)
- Kaye v. Robertson, (1991) FSR 62
- Kharak Singh v. State of U.P., AIR 1963 SC 1295
- Lawrence v. Texas, 539 US 558 (2003)
- Loving v. Virginia, 388 US 1(1967)
- M. P. Sharma v. Satish Chandra, AIR1954 SC 300
- Malak Singh v. State of Punjab, (1981) 1 SCC 420
- Mr. 'X' v. Hospital 'Z', (1998) 8 SCC 996
- Olmstead v. United States, 277 U.S. 438 (1928)

- People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
- People's Union for Civil Liberties v. Union of India, AIR 1991SC207
- Planned Parenthood v. Casey, 505 US 833 (1992)
- R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632
- R.M. Malkani v. State of Maharashtra, AIR 1973 SC 157
- Sharda v. Dharmpal, (2003) 4 SCC 493
- Skinner v. Oklahoma, (1942) 316 U S 535
- Stanley v. Georgia, 394 U S 557 (1969)
- State of Maharashtra v. Madhukar Narayan Mordikar, AIR 1999 SC 495
- State v. Charulata Joshi, (1999) 4 SCC 65
- Thrifty-tel. Inc v. Bezenek, 54 cal rptr. 2nd 468
- Webster v. Reproductive Health Services, 492 US 490(1989)

INTRODUCTION

Development in any field of knowledge provides new avenues in order to cater the needs and to fulfill the aspirations of any civilized society at any given point of time. Advent of technology not only widens its use but also poses anticipated challenges for the legal system and legal universe as a whole. At present, this seems to be very true in relation to Information Communication Technology (ICT) and related development as so called Information Revolution. The Information Technology, as we know it today, has a vast impact on storing information on every conceivable subject of interest to mankind which has transformed the communication system as whole. In real sense, the advancements in Information Technology have been very emphatic, but at the same time, these have negative and devastating impact also covering a wide range of issues of social concern.

In Indian perspective Information Technology related challenges is no longer an illusion but it indicates the prospective impact of the Information Communication Technology as the new frontiers of innovations in criminal activities covering the global perspective through the network of *world wide wave* (*www*) and other sophisticated and improved methods of technology.

In these technology oriented development, the most distinguished and intimate right of any human being is at the stake which is better known as 'Right to Privacy'. The right to privacy refers to the specific right of an individual to control the collection, use and disclosure of personal information. Personal information could be in the form of personal records, habits and activities, family records, educational records, medical records, financial records and intimate communications such as telephonic talks and e-mail.

Further, Right to privacy is also affected in a manner that amounts to violation of public morality and decency in a civilized society with the use of convergence of technologies. The wider application of these innovative technologies has spawned a new and complex set of issues concerning individual privacy and information privacy i.e. data privacy.

The legal implications and standards of law to be observed in relation to protect the socio-cultural and moral norms seems to be inadequate in computer and communication related crimes. Therefore, it is high time to take it as a challenge and to develop the legal framework accordingly. The issue of information i.e. data privacy is also a prime concern to protect the system as well as society. Since, cyber security is a big challenge in current Indian perspective, thus we need a good legal framework in the

area of cyber law, cyber security to protect e-transactions and the common interests of general public at large. In the present Indian legal context, the Information Technology Act, 2000 is a piece make legislation that is weak on the fronts of cyber security and other areas of cyber criminality and thus affecting the privacy rights of Indian citizens and other components of e-governance.

The innovations in communication technology and other way trends of development in Information Technology have gone into creating the fascinating innovations. To communicate with the help of Internet and *www* would not have had the impact that it has had in every sphere of life known to human civilization in prevailing scenario.

At a glance, the existing legal system and framework has shown inadequacy of legal protection dealing with Information Technology in relation to privacy rights. Moreover, the Constitution of India does not grant in any specific and express terms any right to privacy as such. Right to privacy is not enumerated as a Fundamental Right in the Constitution. However, such a right has been culled by the Supreme Court of India from Article 21 and several other provisions of the Constitution read with the Directive Principles of State Policy.

Therefore, the present study is an attempt to bring together various perspectives of information technology and its manifold impact on 'Right to Privacy'. In this study, the Right to Privacy has been analyzed with theoretical, technological and socio-legal perspectives of information technology based system of telecommunication and electronic transaction in modern times.

The importance of the study is critical in order to evolve and to develop proper directional, controlled and systematic measures to protect the most cherished human want of privacy in well accepted and comprehensive manner.

The study has also been directed towards certain and limited glimpse of data protection legislations, conventions and directives covering the issues relating to data protection i.e. data privacy in comparative fashion prevailing in contemporary legal system of the world such as U.S.A., U.K. & European Union (EU) etc. in order to assess the contemporary challenges to law enforcement agencies and tech-based trans border means of communications.

1. THE CHOICE OF TOPIC

The following facts guided the choice:

I. The contemporary legal system is driven by the challenges of advances in science & technology.

II. The advent of Information technology and its applications have its own impact on human beings regarding the safety and security of their right of privacy.

III. The medium of information communication technology have to be regulated and controlled by developing up-to-date legal mechanisms in present system of global networks of communication such as Internet and world wide networks of communication technology.

IV. Indian legal system lacking behind to control the growing menace of cyber based criminality.

V. A viable and effective mechanism is required to control the system with efficient and effective legal frame work.

2. NEED FOR THE STUDY

The need for the present research originates from debatable issue of right to privacy in contemporary development of modern versions of science and technology. This study may fulfill the need and may also provide some valuable contributions to develop the technology based legal system for the benefit of modern civilized society in order to meet out the global perspectives of legal developments. The concern of individual privacy and

information privacy i.e. data privacy has urgent need for research in this challenging area.

3. THE OBJECTIVE OF THE STUDY

The objective is to undertake the present research work:

I. To analyze the development of information technology and its impact on right to privacy.

II. To examine the current and existing legal frame work to protect the right to privacy.

III. To give effect the emphasis on protection of information relating to privacy in this age of Internet and well advanced system of telecommunication.

IV. To develop the new mechanism of regulation and control such as establishment of 'Cyber Regulatory Authority of India' (CRAI) and widening the present ambit of information technology related legislations.

V. To emphasize the advancements and changes in existing cyber practices of regulation and enforcement.

VI. To make cyber legislation more stringent and effective by the making of special laws and constitutional amendments.

VIII. To add and empower the enforcement agencies with proper development of techno-legal courses and personnel such as introduction of models of cyber policing system based on global pattern and high standards of competence.

4. RESEARCH HYPOTHESIS

The present research proceeds on the following hypothesis:

I. Development of information Technology has serious impact on 'Right to Privacy' and the extent is unlimited with constant development of science and technology.

II. The innovation and application of information technology is a developmental process, therefore the legal frame work should also be developed at required pace.

III. The Constitutional provisions and judicial responses in relation to breach of privacy and confidentiality are not so explicit to resolve the malady.

IV. At present the Information Communication Technology (ICT) is a very topical issue not only in India but in the rest of the countries. To meet out the resulting challenges legal mechanisms are to be evolved, developed and proper restrictions to safeguard the individual interest as well as national Interest must be taken.

V. Impact of techno-legal advancement and contemporary requirement of regulation and control of data privacy.

5. SCOPE AND LIMITATIONS OF THE STUDY

The scope is restricted to the following:

I. Technological development and information privacy under the legal framework.

II. Restrictions on information super highways with due importance to information privacy and data privacy i.e. dissemination of personal data.

III. Unlimited possibilities of Internet & *www* and restricted use of data by application of data protection laws.

IV. Regulation and control of information technology to protect the right to privacy.

V. Indian legal framework and control mechanisms of confidentiality and privacy.

VI. Legal limitations and technological implications, difficulties and possible remedial measures.

6. IMPACT OF THE STUDY

The technology has always been the boon or bane to human civilizations and in strict sense to human beings. The subject matter of study is so delicate that it has its own inherent controversies and concerns. Therefore, the impact of the study would certainly helpful to add and to develop the existing legal framework on the subject. However, the adoption of the information technology i.e. Internet and *www* would not have had the impact that it had as so such brain power has involved into creating the problem of abuse or misuse of this fascinating innovation of Information and Communication Technology (ICT).

7. RESEARCH METHODOLOGY

The study is doctrinal and analytical. It is based on comparative and critical study of Constitutional and legal mechanisms in international legal systems particularly U.S.A., U.K. and European Union (EU) and Indian Legal framework relating to information technology. The study has its own limitation due to the impact of constant developing technologies and its applications in this high-tech system of governance and legal developments.

8. CHAPTER-WISE INTRODUCTION

The brief *chapter-wise* contents are, as under:

Chapter-1 pertains to a brief retrospect of Computer and Internet related developments and a summary of Information Technology related legal infrastructure based on *UNCITRAL* model law on electronic commerce in Indian legal framework known as Information Technology Act, 2000.

Chapter-2 deals with techno-legal developments in relation to its impact on right to privacy. The critical study has been included based on the constitutional perspective and case-by-case development as per Indian Judicial response and foreign cases.

Chapter-3 attempts to reflect the issue of Information Privacy (i.e. data privacy) and impact of technology on it. Since, the convergence of technology has special relevance with respect to technology based activities on the Internet thus its consequences in electronic format on data privacy has been highlighted.

Chapter-4 deals with the aspects relating to right to privacy and critical issue of data protection in Indian legal perspective. A brief analysis of relevant provisions of Information Technology Act, 2000 has been incorporated to reflect the current Indian Legal position.

Chapter-5 attempts to give the legal position of right to privacy and data privacy related legislations in various countries of the world such as U.S.A., U.K., The council of Europe, Japan and European Union etc. to provide a concept of data protection and other related issues of trans border flow of information.

Chapter-6 deals with remedial perspectives of individual privacy and data privacy in order to develop a model law on data protection in relation to the current needs of privacy protection.

In the last, conclusion and suggestions have been given to highlight the immense need of improvement in legal infrastructure regarding the protection of individual privacy as well as data privacy with reference to impact of new developments in the area of information technology.

Chapter-1

Computers, internet and the law

CHAPTER-1

Computers, Internet and the Law

An Overview

The Internet is a network of computers linking many different types of computers all over the world. It is a network of networks sharing a common mechanism for addressing and identifying computers, and a common set of communication protocols for communications between two computers on the network. The Internet, an umbrella term covering countless network and services that comprise a super-network, is a global web of network of computer networks.

The Internet has eventually become a link for academic institutions to share researches and then evolved into an instrument for mixed academic, commercial, and personal uses, but even the most visionary original development team member could not have anticipated the phenomenal growth and current state of the Internet.[1] The Internet now provides access to electronic transactions to millions of users.

[1] See http:// info.isoc.org/Internet/history/brief.html

A revolutionary development on the Internet is the *World Wide Web (WWW).* It is a component of the internet that provides access to large amounts of information located on many different servers. The web also provides access to many of the services available on the internet.[2]The fundamental unit of the web is the web page. The pages in text document contain links to other web pages, graphics and audio files, and other internet services such as File Transfer Protocol (FTP) and E-mail.

This chapter has been given in the very beginning of the study with the avowed purpose of making clear certain basic terminology used in the language of computers. It will make the readers very comfortable and convenient in knowing the work of the researcher. A brief perusal of the Information Technology Act, 2000 has also been given.

Evolution of Internet: A Brief History

A modest communication experiment, which was initiated by a team of scientists under a research project in the 1960's founded by the United States Federal Government has resulted in global linked network of computers is known as the Internet. By the end of 1969, four computers were connected together

[2] *Ibid.*

into the initial set up and the saga of the Internet had commenced.

ARPANET[3], the first Internet, was launched in the year 1969. The Internet is a network of computer linking as possible as many different types of computers all over the world. It is also called as network of networks sharing a common mechanism for addressing or identifying computers, and a common set of communication protocols for communications within the network (i.e. between two computer on the network).

As quoted above, the Internet has its root in the *ARPANET* system of the Advanced Research Project Agency (ARPA) of U.S. Department of Defence (USA).[4] *ARPANET* was the first WAN and only four sites in 1969. The first large and successful demonstration of the *ARPANET* occurred at the International Computer Communication Conference (ICCC) in the year 1972.[5] The Internet evolved from basic ideas of *ARPANET* for inter connecting computers, and was used by research agencies, organizations and universities initially to share and exchange information.

---

[3] Developments-The Law of Cyberspace (Editor's Note), Harvard Law Review (Vol. 112) P.1578

[4] See , *American Civil Liberties Union v. RENO*, 929 F. Supp.824 (1996)

[5] This was the first public demonstration of this new network technology to the public.

In 1989, the Government of United States of America (USA) lifted restrictions on use of the Internet, and allowed it to be used for commercial purposes and since then the Internet has grown globally to become the world's largest network allowing almost all nations around the world to communicate with each other.[6] The basic services provided by the Internet to its users are electronic mail (e-mail), file transfer protocol, telnet and use net news.

The World Wide Web

The US Government released the control of Internet in1994 and *WWW* was born. The *World Wide Web* (called *WWW* or *W3*) is the most popular and promising method of accessing the Internet. Main reason for its popularity is use of a concept called Hypertext. Hypertext is a new way of information storage and retrieval that enables authors to structure information in novel ways known as an effectively designed Hyper Text Markup Language (HTML). HTTP was written by *Tim Berners-Lee* in1989, but came online only in 1993.[7]

[6] Keith Webb, "The Internet as an Object of International Interest ", Stephan Chan and Jarrod Wiener(eds.), Twentieth Century International History, 1999, I.B.Tauris Publishers, LONDON, PP.230-232

[7] R. T. Griffiths, "Internet for Historians, History of the Internet",

The WWW uses client-server model and an Internet Protocol called Hyper Text Transfer Protocol (HTTP) for interaction between computers on the Internet. Any computer on the Internet using the HTTP protocol is called a Web Server, and any computer accessing that server is called a Web Client. Use of client-server model and the HTTP allows different kinds of computers on the Internet to interact with each other.[8]

WWW Browsers

To be used as a web client, a computer needs to be loaded with a special software tool known as *WWW* browser (or browser). Browsers normally provide following navigation facilities to help users save time, while Internet surfing (process of navigating the Internet to search for useful information):

1. Unlike FTP and Telnet, browsers do not require a user to log in to server computer remotely, and then to log out again when the user has finished accessing information stored on server computer.
2. Browsers enable a user to visit a server computer's site directly and access information stored on it by specifying its URL (Universal Resource locator)

---

at http://www.let.leidenuniv.nl/history/INTERNET.HTM

[8] *Ibid.*

address. URL is an addressing scheme used by *WWW* browsers to locate sites on the Internet.

3. Browsers enable a user to create and maintain a personal hotlist of favorite URL addressees of server computers that user is likely to visit in future frequently. A user's hotlist is stored on his/her local web client computer. Browsers provide hotlist commands to enable a user to add, delete, update URL addresses in hotlist, and to select an URL address of a server computer from hotlist, when the user wants to visit the server computer.
4. Many browsers have a "history" feature. These browsers maintain a history of server computers visited in a surfing session. That is, they save (cache) in local computer's memory, the URL addresses of server computers visited by a user during a surfing session, so that if the user wants to go back to an already visited server later on (in the same surfing session), the link is still available in local computer's memory.
5. Browsers enable a user to download (copy from a server computer to local computer's hard disk) information in various formats (i.e., as a text file, as an HTML file, or as a postscript file). The downloaded

information can be later (not necessarily in the same surfing session) used by the user.

Implications of Computers and Internet

In the present era of information technology and globalization of trade and commerce, it is not possible for anyone to stay away from the impact of information and communication technologies. Moreover, it has certain transitional and legal implications with the use and application in terms of control and regulations framed for new technology.

New communication systems and digital technology have made dramatic changes in every day transactions. Business transactions are being made, with the help of computers and Internet. Business communities as well as individuals are predominantly using computers to create, transmit and store information in the electronic form instead of traditional paper documents.

Information stored in electronic form is cheaper. It is easier to store, retrieve and speedier to communicate. Since, electronic commerce eliminates the need for paper based transactions; hence to facilitate e-commerce, there is need for

legislative changes i.e. switch over from traditional paper based commerce to e-commerce.

Internet transcends national boundaries. The user in cyberspace[9] traverses a jurisdiction less sovereign region that is not subject to any state jurisdiction. As of now there is no comprehensive legislation on cyberspace jurisdiction[10], any where in the world due to the fact that cyberspace has no specified territorial boundaries.

Indian Information Technology Law

The United Nations Commission on International Trade Law (*UNCITRAL*) adopted in June 1996, a Model Law on Electronic Commerce[11], intended to give states a legislative framework to remove barriers to electronic commerce (e-commerce).

In furtherance of the United Nations, General Assembly *Resolution No. 51/162, dated 30th January, 1997* urging the member states to enact or revise their laws to create a uniform legal environment for the alternative regulating framework to

[9] The term "cyberspace" was coined by 'Norbert Weineer' from the Greek word "Kubernar" Internet virtually creates a world of its own.
[10] Cyberspace is a computer governed environment, which does not exist in reality, yet serves most of the purposes that the real world serves.
[11] Available at http://*www.uncitral.org*/ml-ec.htm

paper based methods of communication, therefore, India being signatory to it has to revise its laws as per the said Model Law.

The Information Technology Bill was passed by both the Houses of Indian parliament, and it received the assent of the President on 9th June, 2000 and became The Information Technology Act, 2000.[12]

The Information Technology Act, 2000(I T Act, 2000) is India's response to regulate the use of computers, computer systems and computer networks as also data and information in the electronic format.

The said legislation has the provisions for the validity and legality of electronic transactions (e-transactions). The I T Act, 2000 has varied nature of provisions pertaining to electronic authentication of records, confidentiality of privacy and information, digital signatures, cybercrimes and liability of network service providers i.e. Internet service providers (ISP's).

From 17th October, 2000, when the I T Act, 2000 came into implementation, the said legislation has confronted with some very interesting perspectives of cyber challenges and cyber criminality. However, certain inadequacies are also at the forefront posing practical difficulties in the implementation of

[12] The Information Technology Act, 2000 (No. 21 of 2000)

the said legislation due to the constant innovations and improvements in technology.

Considering the object and reasons of the I T Act, 2000 following is noteworthy:

"The Act is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communications, which involves use of alternatives to paper based methods of communication and storage of information to facilitate electronic transactions of documents".[13]

Thus, the Act facilitates the way for electronic governance (e-governance) based on the use of information technology in Indian legal system.

The increasing use of information and communication technology has given rise to serious threats of information security and consequently compliance concerns in relation to security policy prescribed for retention of electronic records and security of data.

To prevent the possible misuses arising out of transactions and other dealings concluded over the electronic medium the I T

[13] See, Statement of Object and Reasons, The Information Technology Act, 2000

ACT, 2000 creates civil and criminal liabilities for contravention of the relevant provisions.[14]

A brief Review of I T Act, 2000

The IT Act aims to provide the legal recognition to transactions carried out by means of electronic data interchange and other means of electronic communication, hence to develop the infrastructure for electronic commerce, some of the issues addressed by the I T Act, 2000 include;[15]

- The Act provides that any subscriber can authenticate an electronic record with his digital signature, and subsequently any person can verify that document by using the subscriber's public key.[16]
- The Act states that all electronic records and digital signature have legal acceptance. The chapter also confers rights to the Government to make rules with to digital signatures.[17]
- The Act deals with the attribution, acknowledgement and dispatch of electronic records and digital signatures.[18]

[14] *Ibid.*
[15] See , http//www.nasscom.in/NormalPage
[16] See, Section 3
[17] See, Sections 4-10
[18] See, Sections 11-13

- The Act provides the regulation of the certifying authorities. The chapter also lists the power of the controller to investigate any contraventions to the provisions of the Act.[19]
- The Act provides the condition under which a digital signature may be suspended or revoked.[20]
- The Act states that any person, who accesses, downloads copies extracts data without authorized means or permission is punishable. It also states that any person tampering with, damaging, denying unwarranted access to or manipulating any computer/computer system shall be liable to pay damages by way of compensation not exceeding INR 10 million to the affected persons. Introducing viruses or causing disruptions in a computer are also punishable under the Act.[21]
- The Act describes the role of the Cyber Regulation Appellate Tribunal (CRAT).[22]
- The Act deals with offences such as wrongful loss or damage or destruction of information, deletion or alteration of any information in a computer network,

[19] See, Sections 17-34
[20] See, Sections 35-42
[21] See, Sections 43-47
[22] See, Sections 48-64

'hacking' etc. and prescribes the punishment. It also includes offences such as tampering with computer documents; publishing obscene information, misrepresentation, and breach of confidentiality and privacy.[23]

- The Act states that if a network service provider/intermediary can prove that he has taken diligent steps to prevent the offence he has been charged with, or that it was unintentional, he is not punishable under the Act.[24]

In short, a close perusal of the Information Technology Act, 2000 which contains 94 sections and 4 schedules, it appears that some aspects need improvement in order to protect 'cyberspace'.

To make the information technology a more reliable and safer information enterprise, integrated effort is required to save all legitimate users, otherwise the operation of this critical and vulnerable infrastructure will remain at risk.

[23] See, Sections 65-78
[24] See, Section 79

Chapter-2

The techno-legal developments and right to privacy

CHAPTER-2

The Techno-Legal Developments and Right to Privacy

An Overview

The development of information technology in modern times has special relevance to the law of privacy. The technology has made it possible to bring the private matters of an individual into the public domain, thus exposing the risk of an invasion of space and privacy.

Advances in information technology and tele-communication networks have radically increased the amount of information and data that can be stored, retrieved, accessed and collated almost instantaneously. Technology blurs the boundaries and move towards convergence of techniques ensure that every bit of information is extracted and logged.

The Internet has facilitated this in an unprecedented manner as an information revolution in present scenario. The growth of technology in the modern world can be viewed as an irresistible drive for efficiency, a relentless urge to achieve the maximum production of goods and services with minimum of human effort.

An element of technological injury appears as an inevitable consequence of this advancement, against which the benefits that flow from the technology have to be balanced. A society is a modern society which exploits computer techniques and where the flow of information is greater and easily collected, recorded, evaluated and transmitted.

Thus a society in which the boundaries created to limit the flow of information may be superceded to the detriment of the privacy of the individual. The life of the individual in a society has to strike a balance between freedom and restrictions. It is inevitable that if any society governed by law, there must be a degree of control depending upon the information regarding the past, present and predicted behavior of the individuals and groups in a particular system.

Thus, the state is interested in obtaining the information even at the risk of interfering with individual privacy and it happens because of the recognized and genuine need of the state to protect the national interest against espionage (act of finding out the secret information) and subversive activities towards the state.

The development of science and technology has been used to penetrate and control what the individual may claim to be his private affairs and actions. Attempts at the invasion of privacy

have probably occurred in all civilized societies from but the scope was until recently restricted by the technological limitations on the propagation of light and sound from the individual under surveillance to a hidden observer or eavesdropper.

The invention of the telescope and photography began to broaden the limits of observation and these were widened further by the microphone and telephone but the event that led to the modern explosion of surveillance techniques was the discovery of the electron in 1897 by *J. J. Thomson*. Moreover, this situation changed after the invention which was perhaps more important than the discovery of electron itself. Electronic equipment could, henceforth, be increasingly small, abundant, cheap and not only did this but made individual surveillance equipment easier to obtain and to conceal. It has also made possible the construction of large computers with their great storage capacity of data banks that are themselves now becoming a serious threat to privacy (i.e. data privacy).

Right to Information vis-à-vis Right to Privacy

The concept of an open government is the direct emanation from the right to know which seems to be implicit in the right of freedom of speech and expression conferred under Article 19(1) (a) of the Constitution of India.

However, in India, the right to privacy is not a specific fundamental right but has gained Constitutional recognition. Unfortunately, the infringement of right to privacy is not covered by the expression "reasonable restrictions"[1] to the right to freedom of speech and expression under Article 19(1) (a).

The result of the restrictions being exhaustively enumerated in, that unless a publication that invades the individual's privacy is "immoral" or "indecent", it is not contrary to Article 19 (2). But this has not restricted the activism of the Courts from carving out a Constitutional right to privacy by a creative interpretation of the right to life as enshrined under Article 21 of the Constitution of India.

Coinciding with these legal implications and technological developments a public spirited i.e. a participatory and meaningful law was enacted in India on freedom of information, namely, The Freedom of Information Act, 2002 was enacted to provide for freedom to every citizen to secure access to

---

[1]The *Constitution of India, Article 19(2):* "Noting in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the state from making any law, in so far as such law imposes reasonable restrictions of the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India the security of state friendly relations with foreign state, public order, decency or morality, or in relation to contempt of court, defamation or incitement of an offence."

information under the control of the public authorities, consistent with public interest, in order to promote openness, transparency and accountability in administration and related matters[2], though it never came into force.

Thereafter, on the recommendations made by the National Advisory Council, a more comprehensive law ensuring greater and more effective access to information was envisaged. As a result, the Right to Information Act, 2005 was enacted by the Indian Parliament and it received the President's assent on 15.6.2005.[3]

At the same time, it has also brought into confrontation between the right of the public to know and the right of the individual to be left alone (right to privacy).

Sting Operations and Right to Privacy

Freedom of press started with dissemination of relevant information about public affairs or the happenings that had direct impact on public welfare. But the so called fourth pillar of democracy i. e. media (Print and Electronic media) has overstepped the demarcation that separates the legally

[2] See Government of India, Report of the Working Group on Right to Information and Promotion of Open and Transparent Government, May 1997.
[3] Act No. 22 of 2005,Section 1

permissible contents from illegal one. Therefore, the regulation and control of irresponsible reportage in general and sting operations in particular is highly a matter of great concern. Since, sting operations began with a laudable objective of exposing corruption in high places and degenerated into cheap entertainment, it is from here that a controversy started on misuse of sting operations.[4]

Regarding the right to freedom of press, it is not advisable to put fetters on free dissemination of information, as it forms the very basis of democratic values. It too has to be understood that the privacy of the individuals whose actions are largely in public domain is also protected.[5]

The question of morality might always be a valid question with respect to a public interest; the question should not be put through questionable means. Public interest must not be confused with all sorts of 'interests'. The private life of a person has to be separated from his public life and all his actions that have no bearing on his public affairs and functions must be kept away from media glare. Right to the freedom of press, which implies within the right to freedom of speech and expression, is

---

[4] See, *LAWYERS UPDATE,* "Sting Operations on Deathbed?" , September- 2007 , PP.12-14

[5] *Ibid.*

not an unlimited privilege for its own sake. It is a limited right to be exercised for public good and in good faith. The very important issue involved with sting operations is right to privacy; it is valid point that at a certain point all sting operations do violate right to privacy in one manner or the other because during a sting operation, in all the cases, the person being covered is not aware of the hidden electronic instruments or camera etc. for recording. This means that the person has not given consent to be covered or filmed, without which, in ordinary course, no one has the right to expose any person. Thus, the right to privacy is breached.

However, it may be contented that an illegal act being committed by a public servant during his official duties and abuse of his official capacities are not worthy of protection under right to privacy law. Besides this, when a public servant performing his official duties is covered in public domain. In these cases, public interest seems to be more valuable in comparison to the right to privacy. But in cases where, there is no abuse of power in relation to public offices but about a moral wrong committed by a private individual, the scales would

definitely tilt in favour of the right to privacy.[6]

It is therefore submitted that public interest has to be seen in relation to public duty. If a person has no duty towards general public, his morally wrong conduct is not questionable and not open to public scrutiny unless he violates the law by such conduct. Every individual has a right to make a life of his choice and pursue such things as he thinks fit. This is very essence of all freedoms.[7]

In other words, every individual has an inviolable right to be left alone in his own pursuit so long as he does not do any harm to any other individual or to the society at large. Thus, without right to privacy, right to all other freedoms will be inadequate in relation to the "right to life" as provided under the Constitution of India. Moreover, it is very important that right to privacy is not allowed to be interfered deceptively. At the same time, the right to freedom of speech and expression has also to be maintained to protect the democratic set up.

Privacy is the claim of individuals, groups or institution to determine for themselves when, how and to what extent

---

[6] *Id.* p.13
[7] *Ibid*

information about them is to be communicated to others.[8]

Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among larger groups, in a condition of anonymity or reserve.

Right to privacy is more of an implied obligation. It is the 'right to be let alone'. Hence, 'Right to life', "the Right to be let Alone" has emerged. [9]

The concern for the Right to privacy was shown by Thomas M. Cooley at the end of the nineteenth century when he observed that privacy was synonymous with the right to be let alone[10]. Therefore, privacy as right is the right to be left alone without unwarranted intrusion by government, media or other institutions or individuals.

Thus, In common legal parlance, the right of privacy has one meaning i.e. a legal right to be left alone; the right to live

[8] Westin A F; Privacy and Freedom, 1967 London
[9] Samuel D.Warren and Louis D. Brandies; "The Right to Privacy" 4 Harvard Law Review 193 (1890) [This Article is the first important one on the Right to Privacy.]
[10] The phrase was coined by *Thomas M. Cooley* in his Treatise, The Law of Torts (2nd Ed., 1888)

life free from unwarranted publicity. In wider sense, privacy is the ability of a person to control the availability of information about and exposure of him or herself. It is related to being able to function in society anonymously (including Pseudonymous or blind credential identification).

Privacy Defined

The term "privacy" has been described as "the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and Circumstances to communicate others." [11]

It means his right to withdraw or to participate as he sees fit. It also means the individual's right to control dissemination of information about himself; it is his own personal possession".[12]

In another view, privacy is a "Zero Relationship between two or more persons in the sense that there is no interaction or communication between them if they so choose".[13] Right of

---

[11] Adam Carlyle Breckenridge: "The Right to Privacy" (1971),Quoted in Madhavi Divan, 'The Right to Privacy in the Age of Information and Communications' (2002) 4SCC (J) 12

[12] *Ibid.*

[13] Edward Shills; " Privacy: Its Constitution and Vivissitudes", 2 Law and Contemporary Problems, (Spring, 1996) 31

Privacy, the right of a person to be free from intrusion into or publicity concerning matters of a personal nature called right to privacy.

Privacy is the ability of an individual or a group to keep their lives and personal affairs out of public view, or to control the flow of information about them. Privacy is sometimes related to anonymity although it is often most highly valued by people who are publicly known.

The simplest definition of privacy was given by Judge Thomas Cooley in *Olmstead v. United States*[14], he called it, "the right to be let alone". Invasion of privacy means "an unjustified exploitation of one's personality or intrusion into one's personal activity, actionable under tort law and sometimes under Constitutional law"[15].

---

[14] 277 U.S. 438 (1928). Roy Olmstead was a suspected bootlegger. He was convicted on the basis of wire tapes installed in his office by the Federal agencies. The question before the court was whether the installation of wire tapes violated his Fourth and Fifth Amendment rights. The court held in the negative saying that the Fourth Amendment was not violated because mere installing wire tapes does not constitute a search and seizure. The Fifth against self incrimination was not violated because they were not forcibly or illegally made to conduct those conversations. However, this case was reversed by Katz v. U.S. (1967).

[15] Black's Law Dictionary, 7th Ed. Garner Bryan A.

Redefining Privacy

Privacy often misconstrued as the notion of informational privacy with one sole exception, has been used interchangeably with that of privacy itself. In other words, the doctrine of substantive privacy has been almost completely overlooked. The doctrine of substantive privacy is of comparatively recent origin. What has not been taken into account is that privacy also shields those substantive decisions of individuals in society, which are fundamental to their identity, individuality and existence. [16]

Rubenfield[17] defines privacy as "the right to make choices and decisions" which forms "the 'Kernel' of autonomy". However, going a step further, he introduces the concept of personhood into the doctrine by stating: "Some acts, faculties, or qualities are so important to our identity as persons and as human beings that they must remain inviolable, at least as against the State the right to privacy is a right to self definition."[18] Thus, "where our identity or self definition is at

---

[16] See, Jed Rubenfield; "The Right to Privacy", (1989) 102 HARV. L. REV. 737, 740.
[17] *Id.* p.753
[18] *Ibid.*

stake, the State may not interfere".[19]

Aspect of Personal Autonomy and Right to Privacy

Privacy, in fact, involves at least two kinds of interests i.e. autonomy privacy interests and informational privacy interests. Autonomy interests means interests in making intimate personal decisions or conducting personal activities without observation, intrusion or interference. Information privacy interests means interests in precluding the dissemination or misuse of sensitive and confidential information. Regarding above, both deserves protection.

The right of privacy has been evolved to protect the freedom of individuals to choose whether or not to perform certain acts or subject themselves to certain dimensions. These dimensions are to be defined in personal autonomy, which has culminated into a 'liberty'. However, this 'liberty' is narrowly defined, and generally only protects privacy of family, marriage, motherhood, procreation, and child rearing. The personal autonomy aspect of the right of privacy has limits, although these are always changing. The contemporary approach to the right of privacy, in as much it protects personal autonomy,

[19] Rubenfield; *op. cit.* p.754

combined with ever-changing public opinion on the status of various relationships and activities, makes a succinct statement about the boundaries of the right of privacy nearly impossible. Probably the best known description of privacy is as person's right recognized in a manner to protect personal autonomy.

The measurement of privacy in relation to statement of the right seems to be inadequate when privacy is to be taken as the 'right to be let alone'. Since it is not possible to live in human society without interacting others, and this requires the sharing of personal information.[20]

Thus privacy issue there consists of two elements: (1) A definition of the circumstances in which parties have the right to collect, use and disseminate personal information about others; and (2) A mechanism for preventing collection, use and dissemination outside limits imposed and subject to different views of what information should be treated as private.

Right to Privacy: The Constitutional Perspective

The Constitution of India has not guaranteed the right to privacy as a fundamental right to the citizens but nevertheless

[20] A concept recognized well before the Information Age, See, John Donne; Devotions upon Emergent Occasion (1624) 17
'*No man is an Island, entire of itself*'.

the Supreme Court of India has come to the rescue of common citizens, time and again by construing "right to privacy" as a part of the "right to life and personal liberty". Although not to be recognized as a fundamental right, the right to privacy has gained constitutional recognition in India.

The Courts in India have carved out a constitutional right to privacy by a creative interpretation of the 'right to life'[21] and the 'right to freedom of speech and expression'.[22] The right to privacy is not one of the "reasonable restrictions"[23] to the right to freedom of speech and expression under Article 19(1) (a). Article 19(1) and (2) read as follows:

(1) All citizens shall have the right-

a) to freedom of speech and expression;
b) to assemble peaceably and without arms;
c) to form associations or unions;
d) to move freely throughout the territory of India;
e) to reside and settle in any part of the territory of India;
f) to practise any profession, or to carry on any

[21] The Constitution of India, Article 21: No person shall be deprived of his life or personal liberty except according to procedure established by law.
[22] Article 19 (1) (a)
[23] *Supra* fn.1

occupation, trade or business.

(2) Noting in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the state from making any law, in so far as such law imposes reasonable restrictions of the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India the security of state friendly relations with foreign state, public order, decency or morality, or in relation to contempt of court, defamation or incitement of an offence.

Analyzing the development of privacy laws in India, one can note that these laws evolved basically from two sources i.e. the common law of torts and the Constitutional law. In common law, a private action for damages from unlawful intrusion of privacy is maintainable. Under the Constitutional law, the right to privacy is implied in the fundamental right to life and liberty. The right to privacy emanating from Article 21 of the Indian Constitution must be read together with the constitutional right to publish any matter of public interests, subject to reasonable restrictions.

The Constitution of India does not grant in any specific and express terms any right to privacy as such. Right to privacy

is not enumerated as a Fundamental Right in the Constitution. However, such a right has been culled by the Supreme Court of India from Article 21 and several other provisions of the Constitution read with the Directive Principles of State Policy.

In India, the first mention of the right to privacy was in 1954 where in, *M. P. Sharma V. Satish Chandra*[24] , the Supreme Court while dealing with a question of the legality of search and seizure operations held that, "a power of search and seizure is in any system of state for the protection of social security and the power is necessarily regulated by law. When Constitution makers have thought fit not to subject such regulation to Constitutional limitations by recognition of a fundamental right to privacy analogous to the American Fourth Amendment we have no justification to import it into a totally different Fundamental Right by some process of strained construction". There the Court clearly held that we did not have right to privacy in India.

In yet another case on privacy, as early as1963, *Kharak Singh v. State of U.P.*,[25] Justice Subba Rao held that the concept of 'liberty' in Article 21 is comprehensive enough to include

---

[24] AIR1954 SC 300; 1954 Cri LJ 865
[25] AIR 1963 SC 1295.

privacy and that a person's houses, where he lives with his family is his "castle" and that nothing is more deleterious to a man's physical happiness and health then a calculated interference with his privacy. The Supreme Court held that surveillance by domiciliary visits and other acts under the Regulation 236 of the U.P. Police Regulations was ultra virus with reference to provisions under Article 19(1) (d) and Article 21 of the Constitution of India.

Similarly, In *Govind v. State of Madhya Pradesh*[26], the Supreme Court undertook a more elaborate appraisal of the right to privacy.

In this case, the Court considered the constitutional validity of a regulation which provided for surveillance by way of several measures indicated in the said regulation.

The Court upheld the regulation by ruling that "procedure established by law" in terms of Article 21 was not violated as the regulation in question was "procedure established by law", in terms of Article 21. The court also accepted a limited Fundamental Right to privacy "as an emanation" from Articles. 19 (a), (d) and 21.

---

[26] AIR 1975 SC 1378, (1975) 2 SCC 148

The right to privacy is not, however; absolute; reasonable restrictions can be placed thereon in public interest under Article 19(5).

Thus, Mathew, J., observed:[27]

"The right to privacy in any event will necessarily have to go through a process of case-by- case development. Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech create an independent right of privacy as an emanation from them which one can characterize as a fundamental right, we do not think that the right is absolute."

Further, Mathew, J., Observed on the same point:[28]

"Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and the right of privacy is itself a fundamental right, that fundamental right must be subject to restriction on the basis of compelling public interest."

---

[27] *Id.* p.1385
[28] *Id.* p.1386

In fact, Mathew, J. stated the law in following words:

- Privacy–dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior.
- If the court does not find that a claimed right is entitled to protection as a fundamental right, a law infringing it must satisfy the compelling state interest test.
- Privacy primarily concerns the individual. It therefore relates to and overlaps with the concept of liberty.
- The most serious advocate of privacy must confess that there are serious problems of defining the essence and scope of the right. Privacy interest in autonomy must also be placed in the context of other rights and values.
- Any right to privacy must encompass and protect the personal intimacies of the home, the family, marriage, motherhood, procreation and child rearing.

In *Malak Singh v. State of Punjab*[29] Surveillance was held

[29] (1981) 1 SCC 420

to be intrusive and an encroachment upon the right to privacy.

In the landmark case, R. *Rajagopal v. State of Tamil Nadu,*[30] the Supreme Court for the first time discussed the right to privacy in the context of the freedom of the press. The case concerned the right of the publisher of a magazine to publish the autobiography of the condemned prisoner, "Auto Shankar". The Supreme Court held that the press had the right to publish what they claimed was the autobiography of "Auto Shankar" in so far as it appeared from the public records, even without his consent or authorization. But if the press items went beyond the public record and published his life story, it might amount to an invasion of his right to privacy.

The Court recognized two aspects of the privacy:

(1) the tortuous law of privacy which affords an action for damages resulting from an unlawful invasion of privacy, and

(2) the constitutional right "to be let alone" implicit in the right to life and liberty under Article 21.

Justice B. P. Jeevan Reddy observed that:

(1) The right to privacy is implicit in the

[30] (1994) 6 SCC 632

right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages.

(2) The rule aforesaid is subject to exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including the court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others.

(3) In the case of public officials, it is obvious, right to privacy, or for that matter, the remedy of action for damages is simply not available with respect to their acts and conduct

relevant to the discharge of their official duties. This is so even where publication is based upon facts and statements, which are not true, unless the official establishes that the publication was made with reckless regard for truth. In such a case, it would be enough for the member of the press or media to prove that he acted after a reasonable verification of the facts; it is not necessary for him to prove that what he has written is true. But if they go beyond that, they may be invading right to privacy and then they will be liable for the consequences in accordance with law. Thus, the Supreme Court has asserted that in recent times the right to privacy has acquired Constitutional status and it (right to privacy) has several aspects.

The Supreme Court of India has taken into consideration the U.S. position as well as Article 8 of the European Convention on Human Rights which defines the right to privacy.

Another dimension has been added to the recognition of privacy rights, when in *State v. Charulata Joshi*[31], the Supreme Court held that:

"the Constitutional right to freedom of speech and

---

[31] (1999) 4 SCC 65

expression conferred by Article 19(1) (a) of the Constitution which must includes the freedom of the press is not an absolute right.

The press should first obtain the willingness of the person sought to be interviewed and no court can pass any order if the person to be interviewed expresses his unwillingness. "

Right to Privacy: English & the U.S. Position

The law of privacy in England was evolved earlier than in American law; in fact it was the borrowing from the English case law and creatively interpreting it that the law in America developed. And yet, the law of privacy in England has lagged far behind. One of the earliest reported cases in England, *Albert v. Strange*[32], involved the unauthorized coping of etchings made by Queen Victoria and her husband for their private amusement. The etchings, which represented members of the Royal family and matters of personal interests, were entrusted to a printer for making impressions. An employee of the printer made unauthorized copies and sold them to the defendant who in turn proposed to exhibit them publicly. Prince Albert succeeded in obtaining an injunction to prevent the exhibition. The Court's

[32] (1849) 1 Mac&G25:41ER1171

reasoning was based on both i.e. the enforcement of the Prince's property rights as well as the employee's breach of confidence. This case widely paved the way to develop the law of privacy in the United States.

Lord Denning has forcefully argued for the recognition of a right to privacy:[33]

"English law should recognize a right to privacy. Any infringement of it should give a cause of action for damages or an injunction as the case may require. It should also recognize a right of confidence for all correspondence and communications which expressly or impliedly given in confidence. None of these rights is absolute. Each is subject to exceptions. These exceptions are to be allowed whenever the public interest in openness outweighs the public interests in privacy or confidentiality. In every instance it is a balancing exercise for the Courts. As each case is decided, it will form a precedent for others. So a body of case law will be established."

Yet, the law in England was found to be inadequate in protecting privacy even as late as 1991. In the year 1991, the

[33] Lord Denning: What Next in Law, 93

Court of Appeal decided in *Kaye v. Robertson*[34] , the case concerned a well known actor who had to be hospitalized after sustaining serious head injuries in a car accident. At a time when the actor was in no condition to be interviewed, a reporter and a photographer from the Sunday Sport newspaper unauthorizedly gained access to his hospital room, took photographs and attempted to conduct an interview with the actor. An interlocutory injunction was sought on behalf of the actor to prevent the paper from publishing the article which claimed that Kaye had agreed to give an exclusive interview to the paper. There being no right to privacy under the English law, the plaintiff can not maintain an action for breach of privacy. In the absence of such a right, the claim was based on other rights of action such as libel, malicious falsehood and trespass to the person, in the hope that one or other would help him to protect privacy. Eventually, he was granted an injunction to restrain publication of the malicious falsehood. The publication of story and some less objectionable photographs were, however, allowed on the condition that it was not claimed that the plaintiff had given his consent. The remedy was clearly inadequate since it failed to protect the plaintiff from preserving his personal space and from keeping his personal circumstances

[34] (1991) FSR 62

away from public glare. The Court expressed its inability to protect the privacy of the individual and blamed the failure of common law and statute to protect the right.

The US Constitution has recognized two aspects of the freedom of conscience; religion and speech.[35] Where the substantive right to privacy gives to every individual a degree of independence in making certain kinds of decisions following dictates of his own conscience. The freedom of conscience becomes an important repository of the right to privacy, particularly when the freedom is enumerated in the Constitution. Similarly, the right to freely profess, practice and propagate the religion of one's choice, perhaps one of the most personal of all fundamental choices, without the unwarranted intrusion of the state, is a substantial element of the right to privacy.

In an American case, *Jane Roe v. Henry Wade*,[36]the U.S. Supreme Court considered the constitutionality of a statute criminalizing abortion. The right to privacy was considered to be broad enough to encompass a women's right to terminate her pregnancy owing to the intense emotional, mental,

---

[35] Laurence H. Tribe; American Constitutional Law,(1st Edn.,1978)
[36] 410US 113(1973)

psychological and physical strain which it entails.[37]

The Court has observed regarding the right to privacy: "Although the Constitution of the U.S.A. does not explicitly mention any right of privacy, the U.S. Supreme Court recognizes that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exists under the Constitution, and that the roots of that right may be found in the First Amendment, in the Fourth and Fifth Amendments, in the penumbras of the Bill of Rights, in the Ninth Amendment, and in the concept of liberty guaranteed by the first section of the XIV Amendment and that the right of privacy is not absolute."

Since matters relating to right to privacy have been very widely discussed in U.S.A., the U.S. Supreme Court in this celebrated case has ruled that the right to have an abortion is a part of the fundamental constitutional right of privacy of the woman and the state can interfere with such a right only to promote some compelling interest of the state, e. g. the health of the woman seeking abortion.

The U. S. Supreme Court observed: "The ambit of the

---

[37] *Id.*, p.153

right to privacy also includes, the right to procreate i.e. the right of reproductive autonomy.

In a controversial decision, a similar provision was upheld in *Webster v. Reproductive Health Services*[38]. However, the original Position was reaffirmed in case, *Planned Parenthood v. Casey*[39], where the Court elaborated the consequences of abortion:

"Abortion is a unique act. It is an act fraught with consequences for others for the woman who must live with the implications of her decision; for the persons who perform and assist in the procedure; for the spouse, family and society. The destiny of the woman must be shaped to a large extent on her own conception of her spiritual imperatives and her place in the society.[40]

In *Loving v. Virginia*[41] the US Supreme Court struck down a law which prevented interracial marriages. However, the substantive right to privacy in the context of marriage suffered a substantial setback in *Bowers v. Hardwick*[42] where the US

---

[38] 492 US 490 (1989)
[39] 505 US 833 (1992)
[40] *Id.*, p.852
[41] 388 US 1(1967)
[42] 478 US 186(1986)

Supreme Court denied privacy protection to homosexual activity. The decision was reversed in 2003, in *Lawrence v. Texas*[43] where Kennedy, J. found homosexuals to have the same right as heterosexuals, beginning, in his eloquent judgment, with:

"Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the state is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the state should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct."[44]

Similarly, In *Skinner v. Oklahoma,* [45] the U.S. Supreme Court has characterized the right to reproduce as "one of the basic civil rights of man". The Court struck down a statute which called for the sterilization of "habitual criminals", thus ensuring their inherent right of procreation.

---

[43] 539 US 558 (2003)
[44] Id., p.552
[45] (1942) 316 U S 535

In *Stanley v. Georgia*[46],the possession of obscene material in a man' house was condoned for the reason: " If the First Amendment means any thing, it means that a state has no business telling a man, sitting alone in his house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."

In *Katz v. US*[47] the accused revealed information incriminating himself, in a telephone conversation conducted from a public phone booth. The US Supreme Court considered eavesdropping into a conversation, in spite of the fact that it was conducted in a public phone booth, to constitute a violation of the privacy of the accused. Thus, the mere fact that one discloses financial information on the *world wide web* does not mean that others can tap into that information, and if they do so, it amounts to an infringement of one's privacy, because the channel of communication is restricted to oneself and the seller.

In *Griswold v. Connecticut*,[48] the constitutionality of a state law banning use of contraceptives was invalidated by the U.S. Supreme Court as being inconsistent with the right to

[46] 394 U S 557 (1969)
[47] 389 US 347 (1967)
[48] (1965) 381 US 479

privacy. Upholding the notion of privacy, Justice Douglas held:

'Governmental purpose to control or prevent activities constitutionally subject to State regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms'. Striking down the legislation as an unconstitutional invasion of the right to marital privacy, it was held that the idea is repulsive to the notions of privacy surrounding the marriage relationship.

In *Eisenstadt v. Baird*,[49] a provision affecting unmarried couples was rendered unconstitutional albeit under the equal protection clause, as the evil would be identical and the under-inclusion invidious. The Court expounded, in its equally renowned pronouncement, upon the concept of privacy thus:

"If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child."[50]

---

[49] [1972] 405 U S 438
[50] *Id.*, p.453

The A. P. High Court has observed in *B. K. Parthsarathy v. State of Andhra Pradesh*:[51]

"The right to make a decision about reproduction is essentially a very personal decision either on the part of the man or woman. Necessarily, such a right includes the right not to produce. The intrusion of the state into such a decision making process of the individual is scrutinized by the Constitutional Courts both in this country and in America with great care".

After taking note of above mentioned cases, The Supreme Court has observed in *People's Union for Civil Liberties v. Union of India*:[52] "we have; therefore, no hesitation in holding that right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed 'except according to procedure established by law'. "

In *State of Maharashtra v. Madhukar Narayan Mordikar*,[53] the Supreme Court protected the right to privacy of a prostitute. The Court held that even a woman of easy virtue is

---

[51] AIR 2000 AP 156, at159
[52] AIR 1991SC207,211
[53] AIR 1999 SC 495

entitled to her privacy and no one can invade her privacy as and when he likes. The right to privacy has now become established, but as a part of Article 21, and not as an independent right in itself, as such a right, by itself, has not been identified under the Constitution . The Court has, however, refused to define privacy saying, "As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case".

This means that whether the right to privacy can be claimed or has been infringed in a given situation would depend on the facts of the said case, and the view the court takes of the matter.

Telephone Tapping and Right to Privacy

Telephone Tapping constitutes a serious invasion of an individual's right of privacy. It emanates from the question of Tapping of Telephone in relation to constitutional and legal safeguards. Is it constitutionally permissible in Indian legal system? If so, what are the legal consequences? The Supreme Court has been called to consider these questions in various cases.

In *R.M. Malkani v. State of Maharashtra,*[54] the Supreme Court stated that the telephonic conversation of an innocent person would be protected by the courts against wrongful or high handed interference by tapping of the conversation by the police. But the protection is not for the guilty against the efforts of the police to vindicate the law.

People's Union for Civil Liberties (PUCL) v. Union of India,[55] a public interest litigation (PIL) was filed under Article 32 of the Indian Constitution against the incidences of telephone tapping of political persons, thereby challenging the constitutional validity of section 5(2) of the Telegraph Act, 1885[56] in the light of Article 21 and Article 19(1) (a) of the Constitution of India. The Supreme Court held that telephone tapping a form of "technological eavesdropping" infringed the

---

[54] AIR 1973 SC 157 ; (1973) 1 SCC 471

[55] (1997) 1 SCC 301

[56] The Indian Telegraph Act, 1885 S.5 (2) states : On the occurrence of any public emergency, or in the interest of public safety, the Central or a State government or any other officer specially authorized in this behalf by the central government or a state government may , if satisfied that it is necessary or expedient so to do in the security of the state, friendly relations with foreign state or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, shall be intercepted or detained, or shall be disclosed to the government making the order or an officer there of mentioned in the order.

right to privacy. Justice Kuldeep Singh laid down the rule that telephone tapping which amounted to intrusion into privacy can take place only in the gravest of grave situations where national security is endangered and not otherwise. In usual or normal circumstances, there should not be any phone tapping and the person should not be put under surveillance because he has a right to privacy, which is part of the right to life and is recognized by the Constitution of India.

In the course of its judgment, the Supreme Court referred to the International Covenant on Civil and Political Rights, 1966, to which India is a signatory. Article 17 of the Covenant provides for right of privacy and this provision does not go counter to Article 21 of the Indian Constitution.

Article 12 of the Universal Declaration of Human Rights, 1948, is almost in similar terms. The Court has accordingly interpreted Article 21 in conformity with the International Law.

Right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Indian Constitution. The said right cannot be curtailed 'except according to procedure established by law'. The Right to Privacy by itself has not been identified under the Constitution of India. As a concept it may be too broad and moralistic to

define it. Whether right to privacy can be claimed or has been infringed in a given case would depend on the real facts of the said case. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy". Conversations on the telephone are often of an intimate and confidential character. Telephone conversation is a part of modern man's life and at the same time it is an important facet of a man's private life. Right to privacy would certainly include telephone conversation in the privacy of one's home or office.

Telephone tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law.

Extended View of Right to Privacy

Apart from several personal rights which the Supreme Court of India has spelt out of Article 21, the expansive interpretation 'life' has led to extend the right to privacy. In this context, the Supreme Court has performed a yeoman service by taking cognizance, in a number of cases, of extended versions of right to privacy and added new dimensions to it by various judicial pronouncements.

Recently, in *A. Raja v. P. Srinivasan*,[57] considering the freedom of press in relation to status of right to privacy the court opined that right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy and liable for damages.

In *Mr. 'X' v. Hospital 'Z'*[58], where the appellant's blood was to be transfused to another but he was tested HIV (+) at the respondent's hospital. On the account of this fact, the appellant's proposed marriage to one A, Which had been accepted, was called off. Moreover, he was severally criticized and was also ostracized by the community.

Before the Supreme Court the appellant contended that the principle of "duty of care" applicable to persons in medical profession included the duty to maintain confidentiality and that

---

[57] AIR 2010 Madras 77 (DB)
[58] (1998) 8 SCC 996

the said duty had a correlative right vested in the patient that whatever came to the knowledge of the doctor would not be divulged. The appellant added that for violating that duty as well as for violating the appellant's right to privacy, the respondents were liable for damages to the appellant.

The Supreme Court, while rejecting the appellant's contention's, held that the "right to privacy has been culled out of the provisions of Article 21 and other provisions of the Constitution relating to the Fundamental Rights read with the Directives Principles of State Policy. Right of privacy may, apart from contract, also arise out of a particular specific relationship, which may be commercial, matrimonial, or even political. Doctor-patient relationship, though basically commercial, is professionally, a matter of confidence and, therefore, doctors are morally and ethically bound to maintain confidentiality. In such a situation, public disclosure of even true private facts may amount to an invasion of the right to privacy which may sometimes lead to the clash of one person's "right to be let alone" with another person's right to be informed. The right, however, is not absolute and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others".

"Where there is a clash of two fundamental rights, as in this case, right of privacy of one party as part of right to life and right to lead a healthy life of another party which is also a fundamental right under Article 21, the right which would advance the public morality or public interest, would alone be enforced through the process of court, for the reason that moral consideration cannot be kept at bay and the judges are not expected to sit as mute structures of clay in the hall known as the courtroom, but have to be sensitive, "in the sense that they must keep their fingers firmly upon the pulse of the morality of the day.

In Case, *Sharda v. Dharmpal*[59], It was held by the Supreme Court that the right to privacy in terms of Article 21 of the Constitution is not an absolute right. If there were a conflict between fundamental rights of two parties, that right which advances public morality would prevail.

In *District Registrar and Collector v. Canara Bank*[60], "the exclusion of illegitimate intrusions into privacy depends on the nature of the right being asserted and the way in which it is brought into play; it is at this point that the context becomes

---

[59] (2003) 4 SCC 493
[60] (2005) 1 SCC 496; AIR 2005 SC 186

crucial, to inform substantive judgment; if these factors are relevant for defining the right to privacy, they are quiet relevant whenever there is invasion of that right by way of searches and seizures at the instance of the state."

If one considers the judgments pronounced by the Supreme Court, three situations emerge as described below:

(1) That the individual's right to privacy exists and any unlawful invasion of privacy would make the offender liable for the consequences in accordance with law;

(2) That there is Constitutional recognition given to the right of privacy which protects personal privacy against unlawful governmental interferences and invasions;

(3) That the person's "right to be let alone" is not an absolute right and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others;

Therefore, it would be significant that these situations must be taken care while looking into the issues of breach of confidentiality and privacy in this technology driven era of information technology.

In a recent pronouncement, the Supreme Court of India held unconstitutional and violation of the 'right to privacy' the use of Narco analysis, Brain–mapping and Polygraph tests on accused, suspects and witnesses without their consent.[61]

Forcible interferences with a person's mental processes are not provided for under any statute and it most certainly comes into conflict with the right against self-incrimination.

The result obtained through the involuntary administration of either of these tests come within the scope of 'testimonial compulsion,' thereby attracting the protective shield of Article 20(3) enshrined under the Constitution of India.

The administration of scientific techniques in an involuntary manner to a person violates the prescribed boundaries of privacy; therefore, no one should be forcibly subjected to such techniques.

With the case to case development, the law of privacy has been relegated to a penumbral status and not included as a well-defined right. However, the need for balancing individual interests and public interests in giving effect to the right of privacy appears to be in mind of the judges while laying down

---

[61] See, THE HINDU, May 06, 2010, New Delhi.

the principles.

Thus, it is high time to enact laws to protect privacy which is under siege rather than laws that license intrusion into private affairs. At the same time, it is also required to preserve the tenuous balance between the right of privacy and the fundamental right of free speech, expression and information in this modern era of Information Communication Technologies.

Chapter- 3

Information privacy and convergence of technology

CHAPTER- 3

Information Privacy and Convergence of Technology

An Overview

With Information Communication Revolution (ICR) pacing fast to broaden its horizon, the Internet has become fastest growing means of communication through e-mails, chats, browsing, etc. There is an increasing reliance on computers concerning all facets of life.

With the help of computers and Internet, we obtain many services known as e-transactions such as net banking, e-tickets, ordering food & goods etc., online applications and education as well. All this has changed the structure of the society in a way that the computer today occupies a very important place in our lives. This leads to cyber paradox. On the one hand, the computer and the internet have accorded extreme privacy and on the other hand the same tools of technology allow the gagging of privacy.

Today, information superhighway is not really the safest place to be for the matters of electronic transactions. The cyber world and its related criminal activities have no territorial

barriers, and this makes everything complex because evidence is very hard to collect. As multinational companies and governments join e-market activities i.e. e-commerce and business becomes borderless, their vulnerability multiplies. Privacy in this e-market world would be a major area of concern in the coming years with greater degree of damages.

"Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations."[1]

Privacy as an interest has several dimensions; one of these is the privacy of personal data, better known as 'data privacy' or 'information privacy'.

The right to privacy refers to the specific right of an individual to control the collection, use and disclosure of personal information.

Personal information could be in the form of personal interests, habit and activities, family records, educational records, communication means i.e. telephone and e-mail records, medical records and financial records.

[1] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" ,at http//www.anu.edu.au/Roger.Clarke/Intro.html

In this context, the convergence of technologies has spawned a different set of issues concerning privacy rights and data protection. Thus, innovations in information technology have made personal information easily accessible and communicable.

Need of Information Privacy (Data Privacy)

The need of privacy of personal information (i.e. personal data) is that individuals can lawfully claim that data concerning them should not be available to other individuals and organizations and at the same time, these individuals and organizations should be refrained from control and use of it. Thus, every 'data subject' (i.e. individual) has the desire to control over his personal data and its multiple use.

Modern technological developments and convergence of computers and telecommunications technologies have created an environment in which there is inexpensive and ready access to an ever growing pool of personal information.[2]

The Internet is a rich source of information regarding online users of websites and as a consequence websites collect valuable personal information. Through cookies and tracking

[2] Moor, James H; "Towards a Theory of Privacy in the Information Age", Computers and Society, Vol. 27, No.3, (1997) 27-32

software, activities on Internet are followed and information about personal interests and preferences are gathered.

The data collected proves valuable to businesses because through this it is possible for them to target products and services as well as selling space for advertisements on websites. The modern systems have made it possible for even the smallest of businesses to collect and analyze detailed information about identifiable individuals almost anywhere in the world.[3]

Businesses have a great stake in protecting this private information as individuals do and online activities thrive only when there is trust in business practices and the electronic environment.[4]

A most serious concern is that cyber worms (i.e. computer viruses) can turn everything upside down alone with a laptop as his weapon sitting in a basement or in a bathroom connecting it with a mobile phone, and damages can take place within few seconds. Along with these damages there is harassment in several forms to an individual or a group of people online, breaking all barriers of privacy protection by the use of

[3] Moira Paterson; "Privacy Protection in Australia: The Need for an Effective Private Sector Regime" at http://law.anu.edu.au/publications

[4] Miller, A. R.; "The Assault on Privacy: Computers, Data Banks, and Dossiers" (1971) University of Michigan Press.

integrated information technology devices.

Activities on Cyberspace (Internet) Affecting Information Privacy (Data Privacy)

With the information privacy or data privacy issue at centre stage, hacking, spamming, cookies, web bugs, cyber stalking, phishing, and data mining are important areas of concern where insecurity from the technological developments front arises which poses a real threat in this age of convergence technology i.e. combination or confluence of various technologies and its applications in cyberspace.

Hacking

Hacking is 'unauthorized access' to a computer and refers to access the whole or any part of a computer system without permission. Hackers worldwide attempt to hack into remote computer systems for multiple purposes like eavesdropping, data theft, fraud, destruction of data, causing damage to computer systems, or for mere pleasure or personal satisfaction.

The meaning of the term hacking has evolved over the time but is still applied somewhat variably to a complex mix of legal and illegal activities ranging from legitimate creative programming techniques to illicit lock-picking and

manipulation of worldwide phone, computer systems.[5]

At the basic level, hackers[6] are considered to be learners and explorers who want to help rather than cause damage and who often have very high standards. A hacker may not indulge in vandalizing or maliciously destroying data, or in stealing data of any kind. But the term hacking has acquired dual meaning today and a hacker may variably mean a cyber burglar or vandal, an individual or group who believes in causing malicious harm to a network or computer or to steal information like passwords, credit card numbers, names and address financial information even the account information for the ISP and in short anything stored on a computer.

One example of hacking software is a *Trojan horse* program, in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on a hard disk.[7] *Trojan horse* is snooping software, which may come as an e-mail borne virus. The *Trojan horse* may even be able to hidden file and then when one goes online, upload the file to hacker's computer.

[5]Paul A.Taylor; "Hackers-Cyberpunks or Microserfs ?" In Douglas Thomas and Brian D. Loader, Cyber Crimes 36 (Routledge,2000)
[6] Many call those who break into (crack) computer system "Crackers".
[7] See http:// searchsecurity.techtarget.com

This means that even if you do not keep personal information or passwords on your computer the hacker can still obtain them from the keystroke log he uploaded.[8] One of the most recent use to *Trojan horse* is to cause DDoS (Distributive Denial of Service) attacks. In a DDoS attack, the client commands all of the 'servers' located on individual PCs to attack a single website. Thousands of individuals PCs can be commanded to access a website like eBay or Yahoo at the same time, clogging the site's bandwidth and causing an interruption of services.[9]

The software to do this damage is simple to use and readily available at underground hackers sites throughout the Internet. A tiny program can be downloaded from these sites and then with the push of a button the PCs are alerted to go into action all over the world, sending a simple request for access to a site, again and again scores and hundreds of times a seconds.

Hacking: Indian Scenario

There are several cases registered or unregistered related to hacking, in India. Few examples are: Zeetv.com, goznextjob.com etc., and a notorious group of Pakistani hackers

[8] Deepti Chopra & Keith Merrill; Cyber Cops, Cyber Criminals and Internet, P.286-88
I.K. International Ltd., New Delhi, 2002
[9] *Ibid.*

called G-Force during 2001 hacked many websites of Indian organizations, for example, Indian Science Congress, Asian Age Newspaper, National Research Centre, Agricultural University of Maharashtra, IIM (Ahmedabad), IIT (Chennai), Indian National Information Technical Promotion (New Delhi) etc.[10]

Then in 2002, the website of Assam Tourism Department was hacked by unknown hackers. Here the hackers replaced most of the photography to tourism interest with pornographies.[11]

In 2003, a 24 year old engineer from Delhi earned the dubious distinction of being the first person in India to be convicted for a cyber crime. The case was registered following a complaint from Sony India Limited against the accused. It was alleged that this young man, who was employed at a call centre of the electronics company, managed to chat with a woman in the USA and obtain her credit card details on the pretext of updating her bills. He used the same credit card number and bought himself a colour television and a cordless phone through Sony-Sambandh.com, a Sony Website for the NRIs. The cost of both items was dollars 578. Barbara Campa, the holder of that

[10] Raman Mittal and Neelotpal Deka , "Cyber Privacy" in SK VERMA (ed.), Legal Dimension of Cyber Space, 218-220 (Indian Law Institute ,2004)
[11] *Ibid*

credit card number complained to company that the transaction was 'unauthorized'. After purchasing the items, the accused moved to a new address in Gurgaon. However, a photograph taken by Sony officials when making delivery undid his plan. CBI officials soon traced the transaction to the call centre through IP address. After a seven month trial, the accused finally cracked.[12]

Perhaps, the most shocking instance of hacking in India is, when a 15-year old American boy, with a strange name t3k-9, hacked into the Mumbai based Bhaba Atomic Research Centre (BARC) computer network, soon after the Pokhran nuclear tests during May 1998. He passed on the information to his friend named 'Iron Logik', an 18-year-old immigrant from Serbia, and placed the list of 800 BARC login names and passwords to a hacker channel. Again, a group of hackers who call themselves 'Armagedon' gained access to an Indian Bio-Medical Research facility during 1998 and stolen the test results and internal memos on the possible effects of nuclear tests on the country's environment and civilian population.[13] So, from individuals to e-commerce web sites to the web sites of governmental organizations and their databases may be the targets of hackers.

[12] Hindustan Times, Delhi, February06, 2003, India gets its first cyber convict.
[13] Dr. R.K. Tiwari, P.K. Shastri and K.V. Ravi Kumar; Computer Crimes and Computer Forensic 301-308, Select Publisher, Delhi, 2002

Internet service providers and e-mail servers on the other hand still have a cause of action as they maintain physical space for the servers that are being used and if there is any unauthorized entry with intent to commit an offence, they have a cause of action.

This is because the server is maintained in real space and the data is stored in an electronic medium on a physical storage device, therefore it is chattel and laws of trespass (cyber trespass) may apply. This was seen and observed in *America online Inc. V. LCGM, Inc.*[14] and in the case of *Compu Serve V. Cyber Promotion.*[15] Finally the position of law in regard to the applicability to cyber trespass was settled in the case of *Intel Corporation V. Kourosh Kenneth Hamidi*[16] Where it was said: "For the inference to be actionable under trespass, the respondent must have caused some injury to the chattel or to the petitioner's right in it. Under US (California law), trespass to chattel lies where an international interference with the possession of personal property has proximately caused injury. Similarly, In the case of *Thrifty-tel. Inc V. Bezenek,*[17] a computerized circuit-switching network was violated by hackers

[14] F.supp 2d 444, as cited in Mitchell Waldman J.D. Computers and the Internet. NTS.Am.Jur. 2d Computers & the Internet. 571.
[15] 1962 F.supp.1015
[16] 30 cal rptr.4th 1342
[17] 54 cal rptr. 2nd 468

and the prosecution through a change of trespass to chattel against the accused as above referred cases.

Hacking could result in the violation of an individual's privacy and has been made a punishable offence under the Information Technology Act, 2000.

Section 66 of the Information Technology Act, 2000 that deals with 'hacking', states:[18]

- Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.
- Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

The emphasis for committing 'hacking' under the IT Act is on the effect on the information residing in the computer and any subsequent wrongful loss due to access rather than mere

[18] See , S.66 (1), Information Technology Act, 2000

19 Information Technology Act, 2000, Section 70, states:

access to a computer itself. Hacking of a protected system is punishable under section 70 of the Information Technology Act, 2000.[19]

Spamming

Spamming is another area of concern where cyber privacy is at stake and has become a major problem for all Internet users. Spam is unsolicited e-mail on the Internet and is the Internet version of 'junk mail'. Spamming is a weapon to help abusers, who repeatedly bombard an e-mail message to a particular address or addresses. It refers to sending e-mail to hundreds or thousands of users.

Spam is defined as an unsolicited commercial e-mail or unsolicited bulk e-mail.[20] A prime importance in that the mail is to be unsolicited. A communication is considered to be

---

(1) The appropriate government may, be notification in the official Gazette declare that any computer, computer system or computer network to be a protected system.
(2) The appropriate government may, by order in writing, authorize the persons who are authorized to access protected system notified under sub section.(1)

(3) Any person who secures access or attempts to secure access to a protect system in contravention of the provision of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

20 CERT Co-ordination Center, E-mail Bombing and spamming (http://www.cert.org/techotips/e-mail_bombing-spamming.html)

unsolicited if there is no prior relationship between the parties, and the recipient has not explicitly consented to receive the communication. It can also mean that the recipient has previously sought to terminate the relationship, usually by instructing the other party not to send any more communication in the future.[21] It roughly equivalent to unsolicited telephone marketing calls except that the user pays for part of the message since everyone shares the cost of maintaining the internet.[22]

It is an attempt to deliver a message over the Internet, to someone who would not otherwise choose to receive it. Almost all spam is commercial advertising. From the sender's point of view, it is a form of bulk mail, often to a list obtained from a spambot or to a list obtained by companies that specialize in creating e-mail distribution lists. Potential target lists are created by scanning use net postings, lifting Internet mailing lists or searching the web for addresses. The commercial web sites also gather information with automated searches to retrieve e-mail addresses. They use cookies and get help through data mining.

Suppose, a person wants to buy a washing machine, so he visits a web site selling washing machines. Suddenly, a few

[21] David E. Sorkin; "Technical and Legal Approaches to Unsolicited Electronic Mail", 35 U.S.F.L.REV.325 (2001)
[22] See, http://searchmobilecomputing.techtarget.com.

days later when he browses the web, he gets e-mails containing advertisements for washing machines. So, there is somebody sitting on the other side collecting information about a person without his knowledge. The low cost of e-mail spamming offered for sale with millions of e-mail addresses, coupled with the fact that the sender does not pay extra to send e-mail, has resulted in the current explosive growth of junk e-mail. In many instances, the message may be large and data may be meaningless. The efforts is to consume additional system and network resources, thereby abusing multiple accounts at the target site and increasing the denial of service impact. It annoys and invades privacy and creates online traffic jams. Some states in the USA like Nevada, California, Virginia, Colorado, Maryland, Rhode Island and Washington have passed anti-spamming legislations, i.e. legislations targeting only spamming.

There are several other federal legislations, related to spamming and unsolicited commercial e-mails in the pipeline in the US, which include: The Unsolicited Commercial Electronic Mail Act of 2001, The Can Spam Act of 2001, the Inbox Privacy Act of 1999, The Controlling the Assault of Non-

Solicited Pornography and Marketing Act of 2000, The Internet Integrity and Critical Infrastructure Protection Act of 2000. [23]

In Compu Serve case,[24] the defendant, Cyber Promotions, was an advertising company, which specialized in advertising on the Internet as part of its activities, it regularly sent unsolicited e-mails to various mailing lists. The plaintiff, Compu Serve, a famous online service provider in the USA, whose domain name was used as part of the e-mail addresses of millions of people worldwide. Cyber promotions got relevant data from various places and started sending thousands of e-mails to the servers of Compu Serve, finally going to the individual users of the e-mails, with the result that a lot of space on the consumers' computer was filled with those unwanted advertisements. They complained to Compu Serve and Compu Serve itself was receiving a lot of mail and it contended that mail on its servers created a type of jam. Compu Serve went to the court alleging that the defendants have trespassed on their personal property. The plaintiff predicated a motion for a preliminary injunction on the common law theory of trespass of personal property or to chattels, asserting that defendants continued transmission of electronic message to its computer

[23] See, http://www.llnl.gov/ciac/bulletin
[24] Compu Serve V. Cyber Promotions, 962 F.supp.1015 (S.D.Ohio 1 1997)

equipment constitutes an actionable tort. The court said that the defendants couldn't send unsolicited e-mails without first asking, whether they may send it or not. So, an injunction was granted in favour of Compu Serve and against Cyber Promotions practice of spamming.

In Cyber *Promotions, Inc. V. America Online,*[25] the defendant, America Online, another online service provider in the USA, was receiving the same kind of annoyance from the plaintiff, Cyber Promotions. So, America online complained it to Cyber Promotions and when they did not care for the complaint, America Online did send an e-mails bomb themselves to Cyber Promotions saying that they can do the same to jam the entire Cyber Promotions network. Cyber Promotions went to the court and said that America Online has jammed their servers by sending e-mails. America online said that the plaintiff is the one who first initiated it and we are just replying with the same coin. The court held that Cyber Promotions is guilty in the first place, and they should stop spamming. The issue of spamming has not been directly dealt with in any Indian statute. So, there is an urgent need that a legislation be enacted in this regard.

[25] 948F.supp.436 (E.D.Pa.1996)

Spam is an unsolicited message requiring enough time and effort to get rid off. A regular supply of such spam message would naturally result in considerable annoyance. So, the law of nuisance under tort law can be used for bringing the spammer to book. Under the law of torts, nuisance is supposed to have been caused by an act or omission, whereby a person is unlawfully annoyed, prejudiced or disturbed in the enjoyment of property. It would also directly hamper the interest of the user in his electronic mailbox where he does not expect any interference and encroachment. The result, apart from loss of Internet working hours and thwarting one regular e-mails stream, could be one of mental agony and distress.

Continuous spam could cause disruption, damage or denial of service to a computer. In case any person is receiving a voluminous, regular supply of spam messages, recourse could be had to section 43(d), (e) and (f) of the Information Technology Act, 2000 which make damage, disruption to any computer or data or programme as illegal.[26]

Thus 'spamming' is Internet jargon for the transmission of unsolicited e-mail. Spamming is not just a marketing tool; bulk spamming can be used as an aggressive weapon to disable a

[26] See, Section 43, Information Technology Act, 2000 which provides penalty for damage to computer, computer system, computer network etc.

target's e-mail system by overwhelming it with e-mail and attachments.

Cookies

Websites are increasing day-by-day and most of the websites dealing with e-business are getting technological smarter. They know more about a visitor each time he visits the site. For example, when one visits a website, the computer on the other end records the time of the visit, whether or not he has visited them before when he last visited, what he was trying to find out in that particular web site, his e-mail address, and other customizable information. There is a race to acquire more and more information about the prospective customers and find out their consumption preferences and buying behavior. All this data about a person may be collected without him knowing about it. Most websites achieve this stunning feat with cookies.

A cookie is information that a web site puts on one's hard disk so that it can remember something about him at a later time. More technically, it is information for future use that is stored by the server on the client side of a client server communication. Typically, a cookie records your preferences when using a particular site.

Using the Web's Hyper Text Transfer Protocol (HTTP), each request for a web page is independent of all other requests. For this reason, the web page server has no memory of what pages it has sent of a user previously or anything about your previous visits.

A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. The user can view the cookies that have been stored on his hard disk (although the content stored in each cookie may not make much sense). The location of the cookies depends on the browser. Internet Explorer stores each cookie as a separate file under a Windows subdirectory. Netscape stores all cookies in a single cookies text file. Opera stores them in a single cookies data file.[27]

Cookies are commonly used to rotate the banner ads that a site sends so that it doesn't keep sending the same ad as it sends the user a succession of requested page. They can also be used to customize page for the user based on the browser type or other information that he may have provided the web site. In general, cookies help web sites to serve users better.

However, the existence of cookies and their use is

[27] See, http:// Search Security.techtarget.com.

generally not concealed from users, who can also disallow access to cookies information. Nevertheless, to the extent a web site stores information about you in a cookie that you don't know about, the cookie mechanism could be considered a form of spyware.[28]

'Shopping Carts' are good example of cookies in action. When a user browses a series of web pages for items to buy and finds something he is looking for he adds it to his shopping cart by clicking a button on the page. And later, he can view all these items together.

The most important area of concern is that even though a person communicates through an 'anonymous' connection, the website always knows exactly what's in one's personal shopping cart. It does not matter whether the person clicked away to somewhere and comes back, or even if the person has completely shut down his computer and return days later. The web site still knows who that person is and what he was

[28] Spyware is the technology that aids in gathering information about a person or organization without then knowledge.(In other terms, for use of internet it is called a spybot or tracking software). Spyware is a programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program. Data collecting programs that are installed with the user 's knowledge are not , really speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.

shopping for. This is because, when a person visits the same website again his browser sends the cookie to the web server.

The server can use this information to present him with customized web pages. In that case, instead of seeing just a generic welcome page, he might see a welcome page with his name. Once a site has assigned your computer a unique identification code, it can collect the entire click stream data created by visits using your computer, and associate those data with your identification code. Thus a website can create a dossier of information that is associated with your computer and can use this information to personalize its interaction with you.[29]

Cookies can be used to track people to gain statistics as they go through the web site. Because every time we visit a website, we leave a footprint of personal information about ourselves like our preferences, web sites we visits, our financial matter etc. This rather simple capability has profound implications for the privacy of web site visitors.

While cookies do have uses for both the user and web providers and are even helpful, they can be misused. Beneficial of the user when dealing with a company that has a good

[29] Margaret Jane Radin ; "Privacy Online, in Internet Commerce : The Emerging Legal Frame- work" 548 (Foundation Press, New York, 2002)

privacy in place, it is of questionable value when left open and available to the world at large.

The real problem is with aggregation of data form multiple sources resulting in a user profile. Collected personal information is now being treated as a commodity belonging to the collectors.

Many users do not go beyond the knowledge that cookies exist and websites take advantage of the user's inexperience and collect catalogue and commodity information totally unwarranted.

Indian Legal Position

The Information Technology Act, 2000 does not deal with cookies directly but section 43(b) says that if any person without permission of the owner or any other person who is in charge of a computers, computer network downloads, copies or extracts any data, computer data base or information form such computer, computer system or computer network including information or data held or stored in any removable storage medium, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Cookies are meant to extract data from a computer and if planted without permission, could lead to liability under section 43(b). Further, section 43(c)[30] says that if any person without permission of the owner or any other person who is in charge of a computer, computer or computer network, introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network, he shall be liable. Computer contaminant has been defined as any set of computer instructions that are designed to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network. Cookies would come under the definition of computer contaminant as they are designed to record and transmit data residing within a computer. If a web site sends cookies to a user's machine while he is visiting that web site without his permission, the web site could be held liable under section 43 of the Information Technology Act, 2002.

Web Bugs

Web bug, also known as a web beacon, is a file object (usually a graphic image such as a transparent GIF)[31] that is

[30] See, http:// Searchsecurity.techtarget.com

[31] The GIF stands for graphics interchange format and is one of the two most common file formats for graphic images on the world wide web. The other is

placed on a web page or in an e-mail message to monitor user behavior, functioning as a kind of spyware. The word 'bug' here is being used to denote a small, eavesdropping device and is not a euphemism for a programming error. Rather than the term "Web bugs", the Internet advertising community prefers the more sanitized term "clear GIFs", bugs are also known as "I-by-1 GIFs" "invisible GIFs", "beacon GIF". Unlike a cookie, which can be accepted or declined by a browser user, a web bug arrives as just another GIF on the web page. A web bug is typically invisible to the user because it is transparent (matches the colour of the page background) and takes up only a tiny amount of space. It can usually only be detected if the user looks at the source version of the page to find an IMG tag that loads from a different web server that the rest of the page.[32]

A web bug can send several pieces of information to the server computer, and those includes, the Internet Protocol address (IP address) of the computer that fetched the web bug, the Universal Resource Locator (URL) of the page that the web bug is located on the URL of the web bug image which contains the information to be communicated between the web page visited and the site collecting the data, the time the web

JPEG. On the web and elsewhere on the Internet (for example, bulletin board services), the GIF has become a de- facto standard form of image.

[32] See http:// searchwebservices.techtarget.com/Definition

bug was viewed, the type of browser that fetched the web bug image, and the identification code contained in any cookie that was placed by the server.

Web bugs can be used to provide an independent accounting of how many people have visited particular web site. In addition, advertising network can use Web bugs to collect information on what sites a person is visiting to create a personal profile which is stored in a database server belonging to the advertising network and identified by the browser cookie of the network.

A Web bugs is more powerful than a cookie because of its ability to transmit information to a server other than the one that holds the web page the visitor is viewing. Technological innovations are very fast, and now Web bugs can be found in various other applications like e-mails, documents produced by word processing, spreadsheet, presentation, and other software application.

E-mail messages that display graphics and styled text are constructed out of the same HTML code that constitutes Web pages and are equally capable of harbouring web bugs. Such a bug might consist of an instruction to fetch an e-mail user

transmit information back to the server.[33]

For example, when an e-mail user opens his e-mail inbox and reads the message the web bug can "call home" and it can report back the time and date the user opened it. The sender thereby comes to know this information. Although proponents of internet privacy object to the user of bugs in general, they also concede that Web bugs can be put to positive use, for example to track copyright violations on the *World Wide Web.*

No one is authorized to enter someone's house without his permission. Even if law enforcement agencies need to search a premise, they have to go through a legal process and require search warrant. But through Web bugs a computer can be subjected to search without following any legal procedure what so ever. This is a gross violation of privacy especially at a time when a computer has become the store house of a person's most valuable information and personal data.

If a Web bug is planted in a computer without the permission of the owner of the computer or computer network it could lead to liability under section 43(b) and (c) of the

[33] Supra note 28, p.569

Information Technology Act.[34]

Cyber Stalking

The Cyber stalking is a term used for following a person when the person is surfing the Internet or browsing, where he goes and what he does on the Internet. This is done by an agency to profile a potential customer or by a potential criminal in search of information that can be used to commit crimes. Therefore, cyber stalking is considered as a privacy invasion and if it is done with the intention of committing a crime, the normal laws have to take care of these crimes and related activities. However, laws are yet to be developed for controlling this type of criminal activity i.e. tackle breach of privacy.

The stalking also results in harassment which can be mental, physical, racial, religious, sexual or any other as well. Thus, cyber harassment as a crime also brings as to another related area of violation of privacy of users of the internet i.e. netizens.

In this context, violation of privacy of online transactions is a cyber crime of a serious nature, invading the precious and extremely intimate, touchy area of one's privacy on the cyber

[34] See, Section 43, I T ACT, 2000, Supra note 26

network. Cyber stalking is existent today and only become more and more common as the use of computers, and the Internet increases.[35]

Phishing & Pharming

Phishing and Pharming are the names of false e-mails that deceive a user to reveal personal information. Phishing is way of capturing personal data by identity theft, the act of sending e-mail to a user falsely claiming to be an established legitimate Internet address with a justifiable on usually to verify personal information or private information. This type of e-mail scam is called Phishing.

The e-mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card information, and online banking transactions, that legitimate organization already has. Usually there will be a repercussion stated in the e-mail for not following the link, such as "your account will be closed or suspended".

The website, however, is bogus and setup only to steal user's information and the goal of the sender is to disclose

[35] Nandan Kamath (Ed.); Law Relating to Computers, Internet and E-commerce-A Guide to Cyber Laws, Second Ed. (Updated Reprint 2005), Universal Law Pub. Delhi, p. 338

personal and banking information.

Phishing scams occur when cyber criminals try to get vital information and lure us into providing financial information or data such as bank account number, charge account or credit information.

In Pharming scams, software is planted in computer system which re-directs the user from legitimate websites to scam look alike websites.

Data mining

With the rapid developments in the area of information technology, today databases can range in size into the terabytes. Within these huge archives of data lies hidden information of strategic importance. But, it is difficult to arrive at a meaningful conclusion when databases_are so vast. The latest solution to this problem is 'data mining'. Big and small business organizations worldwide are achieving measurably pay offs from this technology.

There are two main kinds of data mining: descriptive and predictive; Descriptive models describe patterns in existing data, and are generally used to create meaningful sub-group such as demographic clusters.

Predictive models can be used to forecast explicit values, based on patterns determined from known results. For example, from a database on customers who have already responded to a particular offer, a model can be built that predicts which prospects are likeliest to respond to the same offer.[36]

Today data mining is being used to increase revenues (though improved marketing) and to reduce cost (through detecting and preventing waste and fraud). So, while innovative e-organizations are using data mining to locate and appeal to higher value customers, and reconfigure their product offerings to increase their sales, individual privacy is at stake and harassment may continue in different forms. People collect and profile data and data mining is used to extract the last straw, which can we obtained from any relevant or irrelevant data.

In *FTC v. Toysmart.Com, LLC, and Toysmart.Com, Inc.*[37]

Toysmart was the one of the most famous toys' portals on the Internet. Through its web site, Toysmart collected detailed personal information about its visitors, including name, address, billing information, shopping preferences, and family profiles,

[36]http://www.twocrows.com/about_dm.htm.

[37] FTC V. Toysmart.com,LLC and Toysmart.com, Inc., filed in United States Bankruptcy Court for the District of Massachusetts, Eastern Division. Chapter 11 Case no.00-13995-CJK, 2000

which include the names and birthdates of children and had build huge database thereof. In September 1999, Toysmart posted a privacy policy which stated that information collected from customers will never be shared with third parties. There policy stated that :[38] Personal information, voluntarily submitted by visitors to our site such as name address billing information and shopping preference is never shared with a third party.

The policy continued, when you register with Toysmart.com, you can rest assured that your information will never be shared with a third party. But when Toysmart.com went into liquidation, all the assets of Toysmart went to he official receiver. The receiver was in the process of selling all the assets of the company, when he found this tremendous database. So, he wanted to commodity and sell the database as well. Soon thereafter, the FTC learned about possible violation of Toysmart's privacy policy from TRUSTe, a nonprofit privacy seal organization that had licensed Toysmart to display its seal. FTC staff investigated this information and discovered that the receiver was offering the database for sale. The FTC filed a suit against Toysmart and there was an out of court settlement. It was agreed that all the data of Toysmart will not be given to everybody and anybody for a price without consulting the

[38] website http://www.ftc.gov/apa/2000/07/toysmart.htm

persons who are the owners of that data. It is so easy to collect data on computers that nobody could mind it. And once the data is collected it could be put to use to which it was totally unrelated originally when it was collected.

The privacy issues, which arise in this scenario of development of information technology, are different not only in scale but also in their impact and nature related with the use of it.Since, issues related to privacy have a long historical background but in this age of Information Communication Revolution they have assumed greater proportions. Computers not only store huge databases but also have the capability to process them in innumerable ways. Falling into wrong hands, such databases could be misused to jeopardize individual privacy. Therefore, the right to privacy extends over the entire gamut of collection, retention, use and disclosure of information. It stems out of the basic human desire for a secure identity of one's own and to that extent, cannot be denied.[39]

The volume and varying nature of transactions carried out on the Internet are such that the right to privacy must exist at least to a limited extent. Volume and nature of transactions raises the issue of cyber security concerns as to the strategic,

[39] In Schoeman F. D.; Philosophical Dimensions of Privacy, Cambridge University Press. Fried Charles ; 'Privacy'. (1984)

political, social and economic fabric of any state govern by cyber technology.

Information or data privacy must be seen as an important aspect of personal particulars which should not be revealed to unauthorized persons. Thus, the privacy of individuals is certainly a concern of the legal framework in this information age.

In Indian legal framework of cyber regulation, the Information Technology Act, 2000 prohibits unauthorized disclosure of the contents of an electronic record.

However, e-surveillance[40] has become a controversial issue since the Information Technology (Amendment) Bill, 2008 has been proposed, but e-surveillance should not be a substitute for cyber security.

Information Technology Act, 2000 also protects the information privacy interests. It prohibits disclosure of information received by a person in pursuance of the powers conferred under the Act. Disclosure could, however, be made without any penal liability to the law enforcing agencies or pursuant to proper authorization by the prescribed authority or

[40] N.R. Sinha & R.S. Vishal; 'Innovations in Information Systems & Technology' Macmillan Pub. India Ltd.(2009) p.157

with the consent of the concerned person.[41]

In this modern perspective, when means of Information and Communication Technology (ICT) have undergone a radical change, the protective measures of the right of privacy may serve as weapon to ensure confidentiality and privacy in human affairs.

The question of whether personal data has been collected 'legitimately' has central importance in the context of electronic transactions, since it is easy to collect personal data via the Internet without any legal basis to do so within the current legal framework because no treaties and international instruments contains rules regarding the control and regulation of trans border data flow.

It is therefore submitted that the issues like privacy rights, life and personal liberty, right to speech and expressions must be addressed and respected by the information communication technology regulations.

[41] See, Section 72 of the IT Act, 2000

Chapter — 4

Right to privacy and data protection Indian perspective

CHAPTER – 4

Right to Privacy and Data Protection Indian Perspective

An Overview

Today in many fields of human activity information technology has been employed as substitute for some or all of the functions performed by human beings and as consequence, these technically performed functions have the potential to conflict with the fundamental human right of privacy and thus raises a legal concern in an era in which the technology has made all data equally accessible, regardless of the jurisdiction in cyberspace.

In this context, the computer world and The Internet (*world wide wave, www*) are perfect examples for both of the sides i.e. positive effect as well as negative effect globally and its activities in a comprehensive manner such as communications, administration, governance, relationships, financial Services (Banking & Non Banking), medical records and individual information.

With the advancement in technological development, there took place a transition in the standard of crimes. In the

present era, most of the crimes are being done by the single click; the criminals are able to get the secured information. The lust of information is acting as a catalyst in the growth of cyber crimes.

Maintaining of data bases is not as much difficult task as maintaining its integrity, so in this era the most concerned debate is going on to discover a perfect method of data protection. Therefore, it is the very big challenge for the business houses, financial institutions and the governmental bodies so as to give adequate protection to their huge databases. In the absence of any particular stringent law relating to data protection, the miscreants are gaining expertise in their work day by day.

Though this world has simplified our life style but it left certain anomalies in procurement of its object which resulted in involuntary disclosure of data. Many countries other than India have their data protection laws as a separate discipline. They have well framed and established laws, exclusively for the data protection.

Data Protection and Indian Legal Perspective

The Constitution of India has implicitly provided the law relating to privacy under the scope and ambit of Article 21. Its interpretation is found insufficient to provide adequate protection to the data. In the year 2000, effort has been made by the Indian legislatures to embrace privacy issues relating to computer system under the purview of the Information Technology Act, 2000. This Act contains certain provisions which provide protection of stored data.

Moreover, in the year 2006, Indian legislature has also introduced a bill known as 'The Personal Data Protection Bill, 2006' so as to provide protection to the personal information of the persons.

The Personal Data Protection Bill, 2006[1]

Upon the footprints of the foreign laws, this bill has been introduced in the Upper House of Indian Parliament *Rajya Sabha* on December 08, 2006[2]. The purpose of this bill is to provide protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for

[1] http//rajyasabha.nic.in/bills-ls-rs/2006/XCI_2006.pdf
[2] *Ibid.*

commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent and for matters connected with the Act or incidental to the Act. Provisions contained in this Act are relating to nature of data to be obtained for the specific purpose and the quantum of data to be obtained for the purpose[3]. Data controllers have been proposed to be appointed to look upon the matters relating to violation of the proposed Act.

On comparing the Indian law with the law of developed countries the proper requirement for the Indian law can be analyzed. Data are not of same utility and importance; it varies from one another on the basis of utility. So, we require framing separate categories of data having different utility values, as the U.S. have. Moreover, the provisions of Information Technology Act, 2000 deals basically with extraction of data, destruction of data.

Organizations cannot get full protection of data through that which ultimately forced them to enter into separate agreements to keep their data secured. These agreements have the same enforceability as the general contract.

---

[3] *Ibid.*

Despite the effort being made for having a data protection law as a separate discipline, the Indian legislatures have left some lacuna in framing the bill of 2006. The bill has been drafted wholly on the structure of the UK Data Protection Law[4] whereas today's requirement is of a comprehensive Act. Thus it can be suggested that a compiled drafting on the basis of US laws relating to data protection would be more favourable to current legal requirements.

Being one of the most concerned topics of discussion in the modern era, legislatures are required to frame more stringent and comprehensive law for the protection of data which requires a qualitative effort rather than quantitative in modern context of developing technologies.

Information Technology Act, 2000: Some Reflections

Regarding the protection, the Act has various provisions and it also provides certain penalties for violation of the prescribed standard.

The Act provides protection against unauthorized access of the computer system by imposing heavy penalty up to one

[4] The U. K. Data Protection Act,1998

crore.[5] The unauthorized downloading, extraction and copying of data are also covered under the same penalty. It also imposes penalty for unauthorized introduction of computer viruses of contaminants.[6] It also provides penalties for assisting the unauthorized access.[7]

The section 65 provides provisions for computer source code. If anyone knowingly or intentionally conceals, destroys, alters or causes another to do as such shall have to suffer a penalty of imprisonment of fine up to 2 lakh rupees. Thus protection has been provided against tampering of computer source documents.

Protection against hacking has been provided under this Act.[8] As per the provision hacking is defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss or damage will be caused to any person and information residing in a computer resource must be either destroyed, deleted, altered or its value and utility get diminished. This Act imposes the penalty of imprisonment of three years or fine up to two lakh rupees or both on the hacker.

---

[5] Section 43
[6] Cl. (c)
[7] Cl. (g)
[8] Section 66

The Act also provides protection to the data stored in the protected system.[9] Protected systems are those computers, computer system or computer network to which the appropriate government, by issuing gazette information in the official gazette, declared it as a protected system. Any access or attempt to secure access of that system in contravention of the provision of this section will make the person accessed liable for punishment of imprisonment which may extend to ten years and shall also be liable to fine.

The section 72 provides protection against breach of confidentiality and privacy of the data. As per this, any person upon whom powers have been conferred under IT Act, 2000 and allied rules to secure access to any electronic record, book, register, correspondence, information document of other material discloses it to any other person, shall be punished with imprisonment which may extend to two years or with fine which may extend to one lakh rupees or both.

Issue of Privacy & Data Protection

In the context of digital or cyber privacy, the privacy concern exists wherever personally identifiable information is collected and stored in digital form or otherwise. Improper or

[9] See, Section 70.

non-existent disclosure control can be the root cause for privacy issue and breach of confidentiality. Since, Data privacy is the relationship between collection and dissemination of data. The challenge in data privacy is to share data while protecting personally identifiable information. The various types of personal information often come under privacy concerns.

Thus, privacy may be[10]:

- **Life Style**
- **Financial**
- **Data/Internet**
- **Medical**
- **Political**
- **Genetic**

Life style

For various reasons individuals may not wish for personal information such as their religion, sexual orientation, political affiliations, or personal activities to be revealed. This may be to avoid personal embarrassment or damage to one's professional reputation.

[10] See, Dhruv Jain, " The Right to Privacy in India: An Overview" , AIR-June 2009-Journal Section, P.91

Financial Privacy

Information about a person's financial transactions, including the amount of assets, positions held in stocks or funds, outstanding debts, and purchases can be sensitive. If criminals gain access to information such as a person's account or credit card numbers that person could become the victim of fraud or identify theft. Information about a person's purchases can reveal a great deal about that person's history, such as places he has visited, whom they have had contact with, products they use, their activities and habits, or medications they have used. In some cases corporations might wish to use this information to target individual with marketing customized towards those individual's personal preferences, something which that person may or may not agree.

Internet Privacy

The ability to control what information one reveals about oneself over the Internet, and to control who can access that information, has become a growing concern include whether e-mail can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited

collect, store, and possibly share personally identifiable information about users.

Medical Privacy

A person may not wish for their medical records to be revealed to others. This may be because they have concern that it might affect their insurance coverage or employment, or it may be because they would not wish for others to know about medical or psychological conditions or treatment which would be embarrassing. Revealing medical data could also reveal other details about one's personal life.

Physician and Psychiatrists in many cultures and countries have standards for doctor-patient relationships which include maintaining confidentiality. In some cases the physician-patient privilege is legally protected. These practices are in place to protect the dignity of patients, and to ensure that patients will feel free to reveal complete and accurate information required for them to receive the correct treatment.

Political Privacy

Political privacy has been a concern since voting systems emerged in ancient times. The secret ballot is the simplest and most widespread measure to ensure that political views are not

known to anyone other than the voter themselves, it is nearly universal in modern democracy, and considered a basic right of citizenship. In fact even where other rights of privacy do not exist, this type of privacy very much exists.

Genetic Privacy

The concept of genetic privacy has only recently entered in our vocabulary. It is necessary in order to prevent genetic discrimination on the basis of apparent or perceived genetic abnormalities. A person may have some serious repercussions on the revelation of a particular genetic disorder, thus genetic privacy is very important.

Generally, Data privacy issues can arise in response to information from a wide range of sources such as financial transactions, biological information, such as genetic records etc., residential and geographic records, administrative records and policy matters, scientific information and records, security and strategic information.

Technological Means of Privacy Protection

With the recent development of commercially available technology based systems, privacy protection has also moved into the hands of individual users. Users of the Internet and of

some physical applications can employ a range to programs and system that provide varying degrees of privacy and security of communications. On the one hand technology is widely being misused for violation of privacy on the other hand the same technology provides means to protect one's privacy. One of these technologies is digital signature.

All electronic documents can be signed digitally and once signed their secured communication on the Internet is guaranteed as the message gets encrypted. It can not be read in transit by any third party and only the addressee will be able to decipher it. Firewall, another network based technology, is frequently used by computer networks towards the attempts to breach the privacy of a network. A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks.

A firewall is a hardware and software combination used to create security checkpoints at the boundaries of private networks. Suppose, there is network of 50 computers, it must have one point from which the information comes in and goes out. At that point a firewall is the form of a checkpoint. It can block traffic to and from suspicious destinations.

The Right to Privacy, Encryption and Cryptography

The use of Internet has provided a new forum to express the views and concerns on a worldwide platform. The freedom to speak and communicate is the fact which demands state interference in public as well as national interest which immediately raises the debatable issue of right to privacy.

At the same time, it is common concern that liberty cannot thrive without certain restrictions put on them so that each individual in society can be best protected from intrusion by the others as well as state also.

It would therefore seen that a technology is required to legitimate utilization of the right to freedom of speech and expression and the right to have a private conversation without intrusion. For this, encryption may provide a practice tool. Since, the practice of encryption and its study that is known as 'cryptography' provides individuals with means of communication that no third party can understand unless specifically permitted by the communicators themselves.[11]

[11] Nandan Kamath; Law Relating to Computers Internet & E-Commerce- A Guide to Cyber laws &The Information Technology Act,2000, Second Edition, Reprint 2005, Universal Law Pub. Delhi, P.367

The technique 'Encryption' is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. Therefore, this has the effect of ensuring total privacy even in open networks like the Internet. In process, encryption involves the use of secret codes and cipher to communicate information electronically from one person to another in such a way that the only person so communicating would know to use the codes and ciphers.[12]

On the other side, the field of cryptography deals with the study of secret codes and cipher and the innovations that occur in the field. Cryptography is also defined as the art and the science of keeping messages secure.[13]

In concern to the right to privacy, it is usually agreed upon that in most democratic countries there is existence of private and public spheres in every citizen's life and that these two spheres are distinct and to be treated as separately.

Although, the line of demarcation is sometimes blurred and continues to be the subject of private as well as public importance such as pornography, public and personal security,

---

[12] See,*Daniel Bernstein v. United States*(Dept. of State), 922 F. Supp.1426(N. D. Cal.1996)

[13] Jonathan Rosenoer, " Cryptography and Speech" at http://cyberlaw.com/1095.html

national security etc. In contrast the liberal democratic state has no power to interfere with the private aspect of its citizen's lives.

There is also a common misconception that the right to privacy is merely a weapon to ensure confidentiality in human affairs. However, this does not reflect the correct and complete picture in the subject matter.

It is important to note that the right to confidentiality arises only after information regarding human transaction or affairs have reached to third parties.

It may be stated that privacy involves the right to control one's personal information and how that information should be used and obtained which is sometimes to be referred as the right to "informational self determination".[14]

With the onset of the Internet and e-commerce and the varying nature of the transaction carried out on the Internet are such that the right to privacy must extend at least to a limited extent.

At the same time, volume and the nature of transactions also raises the issue of various types of computer related crimes

[14] See, A. H. Robertson, "Privacy and Human Rights", 1st edn. (1973), Manchester University Press, Manchester.

e.g. distribution of sensitive information, e-mail scams, password attacks, I.P. Spoofing hacking, credit card frauds, alteration and destruction of digital information etc. which raises the issue of national security concerns as to the political, social and economic health of any country in the present scenario of global menace of terrorism and practice of on-line transactions.

Techno-Legal Safeguards (Encryption)

An encryption algorithm transforms a plaintext into an unreadable ciphered text (encryption) and vice versa decryption using a special key. The economics behind encryption is to transform the problem of keeping thousand of messages secret into the problem of keeping a single key secret.[15] A useful distinction can be made between symmetric and asymmetric encryption algorithms. Symmetric algorithms use the same key for encryption and decryption and decryption. This means that communication parties have to agree on a secret key in advance the disadvantage is this they have to find a secure way to exchange this key. This is particularly cumbersome in an open environment with many participants that may not know each other beforehand. This disadvantage is avoided in asymmetric

[15] G. Aruna Kranthi, "Money in Electronic Age " Published in 'Cyber Space And The Law- Issues And Challenges' NALSAR University, Hyderabad Publication 2004, P.140

encryption methods that use different keys for encryption and decryption. At present, encryption provides the most important tool to keep electronic communication and electronically stored documents confidential.[16] Although new technologies will emerge sooner or later, it can be expected that encryption will remain the cornerstone for most confidentiality services on open network for the foreseeable future. Encryption has a long tradition in the defense area. However, encryption technologies are increasingly integrated into commercial systems and applications.[17]

The above examples already show that the exclusive character of encryption belongs to the past. They also show that increasingly encryption technology is integrated into products primarily to protect, for example, intellectual property rights or to avoid fraud. Moreover, the fast growth of the Internet will create a fundamental change in the use of encryption, it will become an integral part of personal and business computing. Computer stores sell cryptography product and more and more people simply download encryption software from the Internet which can be easily installed on a normal computer system. The integration of complete cipher machines on smart cards is a

[16] *Ibid.*

[17] Digital Mobile Telephones enjoy stronger protection, uses encryption. Pay-TV & DVD also uses encryption.

reality. Computer System could be delivered with standardized smart card readers and fast crypto-chips. Various universities in the world teach cryptology and hundreds of companies in Europe and even more worldwide develop, produce and sell products and systems to be used for encryption.

Electronic commerce and many other applications of the information society will only expand and unfold their economic and social benefits if confidentiality can be assured in a user-friendly and cost-efficient way.[18] Cryptographic technologies are flexible, support a wide range of applications and minimize transaction costs on open networks. Continuous progress in digital technologies will make computing crypto-algorithms even more cost-efficient. European companies have developed substantial capabilities to integrate high-quality cryptographic features into their products and services. As demand for products with encryption is now growing very fast worldwide, it provides substantial opportunities for the industry and job

[18] When using services such as tele-shopping or tele-banking, the consumer needs to be ensured that personal data such as credit card numbers are kept confidential.

- Data protection laws require safeguards like encryption to ensure privacy.
- In storing select secret data and in carrying out sensitive business communication (project details, biding information, research results, etc.) over open networks, companies wise to be protected against industrial espionage.
- Health care tele-matic applications must not allow for disclosure of medical histories of patients to unauthorized persons.

creation in Europe. Furthermore, the application of cryptographic products and services will have an enabling effect in all sectors of economic and social activity. Without this wide scale deployment, the ability to create new, more competitive forms of business and new forms of social interaction will be substantially inhibited.

International treaties, Constitutions and laws guarantee the fundamental right to privacy including secrecy of communications.[19] Consequently in the current shift from offline to on-line information flows, the public needs to have access to technical tools allowing effective protection of the confidentiality of data and communication against arbitrary intrusions. Encryption of data is very often the only effective and cost-efficient way of meeting these requirements. Therefore, the discussion about the prohibition or limitation of the use of encryption directly affects the right to privacy, its effective exercise and the harmonization of data protection laws in the effective implementation.

[19] Art. 12 of Universal Declaration of Human Rights, 1948 ; Art. 17 of International Covenant on Civil and Political Rights (ICCPR); Art. 8 of European Convention for the Protection Human Rights and Fundamental Freedoms, 1950.

Regulation of Encryption: Some Comparative Positions

Concerns over foreign threats to national security have been the primary motive for regulation and control. Whilst countries want to protect their own military and diplomatic communication through encryption, the objective of control is precisely to deny similar benefits of cryptography to foreign opponents, in particular if they do not have equivalent technical means. Therefore, regulation and control mechanisms are in general designed to prevent international proliferation of certain encryption technologies.

Law enforcement authorities and national security agencies are concerned that wide-spread use of encrypted communication will diminish their capacity to fight against crime or prevent criminal and terrorist activities. For this reason, in several member states consideration is being given to how their encryption policy could develop in the future. This has led to national and international discussions about the need, technical possibilities, effectiveness proportionality and privacy implications of such a regulation.[20]

[20] Existing regulation within the European Union and the OECD, Whist export control measures are internationally widely applied, up to now, domestic control of encryption is quite exceptional. In fact, currently only one Member State of The European Union (France), applies a comprehensive cryptographic regulation (Loi N" 90-1170 of 29.12.90, JORF 30.12.90; Decret N' 92-1358, 28.12.92, JORF 30.12.92;

Regulation of use would mean to rule the use of encryption without an authorization as illegal. Alternatively or additionally, supply and control of encryption products and services could be brought under an authorization scheme. Authorization would either be denied or granted under certain conditions, for instance to use only weak encryption or to sell approved software. These conditions are scaleable to satisfy any perceived needs of law enforcement and national security agencies. Such regulations could limit the use of encryption. In addition, divergence between regulatory schemes might result in obstacles to the functioning of the regulatory mechanism in particular for the free circulation.[21] Today, nobody can be totally prevented from encrypting data.[22]

Delivery, exportation and use of cryptography are subject to previous declaration if the cryptography can have no other object than authenticating communications or assuring the integrity or transmitted messages, and previous authorization by the prime minister in all other cases. This law is currently being modified. Although there have been discussions in other Member States, only the United Kingdom has so far launched a Public Consolation on regulation of TTPs for the provision of encryption services (but not for use of encryption)

[Licensing of TTPs for the provision of encryption services-DTI Public Consultation Paper on detailed proposals for legislation. 3.1997]

[21] If any encryption software company which can freely develop its products in its home country, must comply with specific technical or legal requirements in other Member States , this company has to produce at least two , if not more, different versions of its encryption software. The same situation occurs if enterprises want to offer cross-border encryption services.

[22]Criminals or terrorists can also use encryption for their activities. Most of the criminal cases involving encryption that are quoted as examples for the need of regulation concern "professional" use of encryption. It seems unlikely that in such

Firstly, because the access to encryption software is relatively easy, for instance by simply downloading it from the Internet.

Secondly, it is difficult to prove that a specific person has sent an unauthorized encrypted message. Electronic communication on open network is not like an and-to-end telephone conversation where people can be identified for instance by their voice.

Thirdly, encryption is also possible using steganographic methods. These methods allow one to hide a message in other data (e.g. images) in such a way that even the existence of a secret message and thus the use of encryption cannot be detected. As a result, restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not however prevent totally criminals from using these technologies.

The Legal Accession to Encryption Keys underlying principle of this approach is to require that products and service incorporating encryption allow access to the respective keys.

---

cases the use of encryption could be effectively controlled by regulation; *see also "Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism" by DE Denning and W.E Baugh,Jr.*

This would permit regulating agencies to decrypt a ciphered text otherwise difficult or impossible to crack. Different technical and institutional ways to provide key access are being discussed. The two most know concepts are *key escrow* and *key recovery*. Broadly speaking, these concept imply that copies (*escrow concept*) or information (*recovery concept*) about relevant keys are give either directly to regulating agencies or to Trusted Third Parties (TTPs).

(1) Key access schemes are considered by law enforcement agencies as a possible solution, to cope with issues like encrypted messages. However these schemes and associated TTPs raise a number of critical question that would need to be carefully addressed before introducing them.[23]

[23] The ongoing discussion of different legislative initiatives in the US is an illustrative example of the implied controversy. The most critical points are vulnerability, privacy, costs and effectiveness:

- Inevitably, any key access scheme introduces additional ways to break into a cryptographic system (See for a comprehensive analysis the recently published study "The Risks of Key Recovery, Key: escrow, and Trusted Third Party Encryption"). More people will know about "secret keys" and "system designs" leading to higher risks of insider abuse and the TTPs itself can become target for attacks.
- These new vulnerabilities are complex and need to be understood as substantial liability and privacy questions are implied. The costs associated with key access schemes can be very high. Up to now, questions on costs and who would bear them have not been addressed by policymakers. Important cost factors would be the specific requirements put on TTPs, e.g. response time to deliver keys, storage time for session keys, authenticate

Furthermore substantial and unknown costs would occur through the need for scaleability of key access schemes i.e. making it work in a multi million user environment. Up to now, such systems have at best been developed for small scale use.[24]

(2) Any involvement of a third party in confidential communication increases its vulnerability. The main reason for involving a third party in the management of keys for confidentiality is to allow that party to make the keys available to other than the two communicating parties, for example, to law enforcement. Users may therefore not see many advantages

---

requesting government agency, secure transfer of recovered keys, internal security safeguards, etc.

[24] The costs to make them work on an economy of even global wide scale need to be looked at carefully.

- Key access schemes can be easily circumvented-even if, hypothetically speaking, everyone would be forced to pass through these systems.
- Users could first encrypt the data with an unrecoverable key and later use a licensed escrowed encryption system. Unless encryption as such is forbidden, this would even be legal. Anyhow, such an operation could only be detected when an agency actually tries to decrypt the data. It is impossible to "scan" the network to detect the use f non- escrowed encryption. Therefore, use of non-escrowed encryption would not even be able to act as a general indicator for possible illegal activities.
- Users could encrypt a relatively large number of session keys in a way that the previous key encrypts the next one, always using one or several official escrow/recovery systems. Only the last key would be used to encrypt the message. An agency would need to reverse this process and to obtain all keys in order to read the message; although technically feasible, this task would be extremely difficult to manage. To be noted, the uses would have fully complied to a key recovery scheme.

in using TTPs for confidential communication, and probably not even for stored information. Regulators would thus need to offer incentives to convince user to use licensed TTPs for confidentiality purposes, for instance through a "public security label" or even by introducing a "mandatory scheme".[25]

Privacy considerations suggested not limiting the use of cryptography as a means to ensure data security and confidentiality. The fundamental right of privacy has to be ensured, but may be restricted for other legitimate reasons, such as safeguarding national security or combating crime, if these restrictions are appropriate, effective, necessary and proportionate in order to achieve these other objectives. The EU Data Protection directive harmonizes the conditions under which access to personal data, their processing and transfer to third countries is lawful.[26]

Cryptography is one important technical means by which data integrity and their confidentiality can be ensured. To ensure also the secured flow of personal data throughout the regulation,

[25] *Supra, note 15*, P.145

[26] As regards data security the Directive requires Member States to provide that a data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

such technical means must be able to "travel" with the personal information they are securing. Any regulation hindering the use of encryption products and services throughout the regulation and control system thus hinders the secure and free flow of personal information and the provision of related goods and services.

Encryption and Cryptography: A Comparative View

Proposals for regulation of encryption have generated considerable controversy. Industries express major concerns about encryption regulation, including key escrow and key recovery schemes.[27] Although there is a lack of experience, as electronic communication and society, a preliminary examination and assessment can be made in order to build a common understanding of the subject, in particular as member states may have different views on security issues implied. Such an understanding could be founded on the following points:

Problems caused by encryption to crime investigation and the finding of evidence are currently limited, but they may increase in the future. As with any new technology, there will be abuse of encryption and criminal investigations will be hindered

[27] See, Industrial Declaration of the Bonn Conference, July 1997.

because data was encrypted. However, widespread availability of encryption can also prevent crime. At present, the damage caused by electronic crime (e-crime) is estimated in the order of billions of dollars industrial espionage, credit card fraud, toll fraud on cellular telephone, piracy on pay-television encryption. Criminal cannot be entirely prevented from having access to strong encryption and from bypassing escrowed encryption. Benefits of regulation for crime fighting are therefore not easy to assess and often expressed in a fairly general language. However, control measures could make use of encryption for criminal activities more difficult and cumbersome.

In the information society, citizens and companies will increasingly carry out more aspects of their lives and business on-line through tele-conferencing, tele-shopping, tele-working, electronic payment, e-mail, etc. a huge amount of information will be available electronically, in a way never experienced before. Therefore, if citizen and companies have to fear that their communication and transaction are monitored with the help of key access or similar schemes unduly enlarging the general surveillance possibility of regulating agencies, they may

prefer remaining in the anonymous offline world and electronic commerce will just not happen.[28]

Key escrow-or key recovery raises a number of practical and complex questions that policy makers would need to solve in particular issues of privacy vulnerability, effectiveness and expenses if at all required, regulation should be limited to what is absolutely necessary. Regulation would also need to distinguish between a multitude of possible key types (storage keys, session keys, authentication keys etc.) as there are important differences in their use.

Cryptography in India: The Information Technology Act, 2000

The use of cryptography and encryption in India is a relatively new phenomenon. The use of technology in itself, for the purposes of communication, has begun only over the last few years in India. The use of the Internet is a phenomenon of the mid-90s.

According to a recent report[29], in India, there are very few companies involved in the development of tools for

[28] See, Euro barometer opinion survey 46. 1 on Privacy in the Information Society, January 1997.

cryptography. Further, cryptography remains, by and large, within the domain of the defence sector. It was only as late as 1995 that India introduced a list of items that required licensing before export. The list only included encryption software for telemetry systems in specific and did not relate to encryption software in general.

Under a recent agreement between India and US, the former has agreed to facilitate the import of items listed on the US Munitions List (USML)[30]. This, as we have seen earlier, might require specific licensing both for exports and imports.

The Information Technology Act, 2000 introduced some form of control over the use of encryption for communication in India.[31]

The Act takes into consideration the system of 'key-pair encryption' for the recording and authentication of digital signatures. The Act provides specifically, that the public key is to be deposited with a certifying authority.

---

[29] "Cryptography and Liberty 1999: An International Survey of Encryption Policy", at http://www.gilc.org/crypto/crypto-survey-99.html.

[30] The List reads as "Cryptographic systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems" 22 U. S. C. 2278 (a) (1).

[31] See, Chapter III,IV and V of The I T Act,2000

Section 69 of the Information Technology Act, 2000 deals with this problem.[32] This Section provides the Controller of Certifying Authorities with the power to intercept any transmission if certain criteria are satisfied. One such criterion provided for is the security of the state and concerns about the sovereignty and integrity of the nation. In such a case, the subscriber is under an obligation to decrypt the information for the authority. The viability of this provision however, remains questionable. The section provides that the controller can call upon any subscriber to decrypt a message in the event of requirement. Thus, in the absence of any non co-operation from the subscriber, even the controller cannot directly intercept and decrypt a message, since he is only a repository of the public keys and not of the authority is made punishable under the

[32] I T Act,2000; Section 69 reads as under:

Directions of Controller to a subscriber to extend facilities to decrypt information.-

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section(1), extend all facilities and technical assistance to decrypt the information

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

section. Thus, it is only for encrypted messages. Since, the controller cannot directly decrypt messages the right to privacy is still protected to a large extent.

It will be seen that complete discretion is vested with the controller to determine whether a condition has arisen where a transmission may be intercepted in the interest of national security. The right to an encrypted transmission may be viewed as integral to the right to privacy flowing from article 21 of the Constitution. In such a case, the right can only be curbed by a "procedure established by law." It is now well settled that such a procedure must be right, just fair and reasonable to be valid.

One cannot deny that there arise exceptional circumstances when transmissions need to be intercepted to prevent anti-national activities. But such circumstances cannot be abused to further political vendetta. On a plain reading of section 69, it may be concluded that the procedure is not adequate as it leaves complete discretion in the hands of the controller. The wording, it may be pointed out, is similar to that of the Telegraph Act, 1885, that came up for discussion in the *P.U.C.L.* Case[33]. If one follows the ruling in that case, it may be

[33] *P.U.C.L. V. Union of India* (1997) 1 SCC 318

said that inadequate procedural safeguards would render the section inapplicable.

Further, considering the fact that the section also provides for punishment in the event of non-compliance, it is imperative that stronger safeguards be built into the system. Thus, the question as to what constitutes a security threat or when the friendly relations are being threatened should not be left to the sole discretion of the controller, but must emanate from the legislature. In the alternative, the controller should frame specific regulations under Section 89, laying down specific criteria s to when the security of the nation is being threatened and the like. In the absence of such measures, the provision in Section 69 can be said to be an infringement of the right to privacy in view of Article 21 and, consequently, unconstitutional and void *ab initio*.[34]

As in the case of any issue affecting constitutional rights, the validity, or alternatively, the invalidity, of restrictions on the practice of cryptography and encryption remains mere speculation. True, the right to privacy is recognized as inherent in the right to life with dignity in Article 21 and the right to freedom of speech and expression in Article 19. Neither of these

[34] Nandan Kamath; Law Relating to Computers, Internet and E-Commerce-A Guide to Cyber Law , Universal Pub. Delhi (Reprint ,2005) P.391

can and should be allowed to stand as an impediment in curbing activities prejudicial to national security and interests. Not surprisingly, both these rights contain express conditions when they may be deprived.[35]

At the same time, the balance cannot be allowed to till completely to one side, so as to negate the basic liberties, even when not absolutely essential. The only way out is a compromise between the two extremes. While the restrictions on cryptography and encryption may be abused for several illegitimate purposes, so also the freedom is liable to be misused for anti-national activities. The solution lies neither in absolute freedom nor unwarranted state control.[36]

A possible solution to the problem may lie in the technology that encryption uses. The problem has to be looked at, at a two-fold level. At one level, the issue is of encryption and cryptography as a mode of free speech and at the other, is the more important issue of cryptography as an integral part of the right to privacy. While the former may be subject to reasonable restrictions, the second may be restricted only by a procedure established by law.

---

[35] *Ibid.*
[36] *Ibid.*

With regard to the issue of free speech, it would be only reasonable to adopt the standard applied by the courts in permitting restrictions on other modes of expression. Cryptographic studies should therefore be dealt with as any ordinary publication and restraints on the same should be allowed only in so far as Article 19(2) of the Constitution of India permits them. With regard to the issue of privacy and the deprivation of the same by a procedure established by law, the answer lies in a strong and comprehensive set of safeguards to ensure that state interference is permitted only when absolutely essential.[37]

It may not be unreasonable to build procedural safeguards into the existing IT Act, 2000. Such safeguards would have to include procedures for declaring when an issue involving national security concerns has arisen and on what concerned authority should be allowed to intercept encrypted information and be permitted to decrypt the same. Such a proclamation is not to be invoked at the absolute discretion of the authority; it will have to be made by the concerned legislature.

Further, by making such a proclamation, a provision could also be made to provide that for the period of the emergency or

[37] *Id.* p.392

security concern, encryption should be avoided. In spite of this, if encryption is carried on, the government should have the authority to intercept the same. This would have the dual effect of avoiding unnecessary breaches of privacy and also reduce the task of the government in intercepting and maintaining records substantially.[38]

Moreover, in addition to a general invasion of privacy possible through the process set forth above, it may also be necessary, as mentioned earlier, to intercept the messages of specific individuals, even when an actual emergency is not proclaimed. In such a scenario, it would be both unreasonable and impractical to require a proclamation by the legislature. However, here too, the circumstances necessitating the invasion will have to be clearly set forth by the relevant authority and the procedural guidelines as to maintenance and destruction of intercepted message will have to be adhered to. While this would give the authority concerned the power to single out an individual, it nevertheless will still be subject to review by an advisory board, as laid down in the *P.U.C.L.* Case[39] and later, if necessary, by the judiciary, arbitrary action would be reduced. Another alternative might be the process of prior judicial

[38] *Ibid.*
[39] *Supra*, note 33

permission, before the actual passing of the order. However, this approach has several practical problems and may not be appropriate, when action needs to be taken immediately.

When an interception is to take place, the same will have to be done with certain specific guidelines. Detailed records and copies of the intercepted messages should be kept and destroyed once the proclamation is no longer in force. The cryptographic keys obtained should be similarly deleted from government resources to ensure that authorities can no longer use them to intercept messages, in the absence of any emergency.

It is true that no procedure is completely foolproof and without loopholes, the procedure outline above gives individuals the choice to avoid the usage of encryption for a specific period and, thereby, avoid any breach of their privacy. While the executive should work out the exact nature of the guidelines and procedures, the aforesaid scheme may provide a starting point to develop the mechanism of control and regulation to protect the privacy and confidentiality.

However, it has to be contemplated in a true democratic set up where liberties of individuals are supreme to function, mere legislative protections in the absence of a strong political will, would be futile. Therefore it is submitted that the legal

infrastructure should be developed and enlarged without any delay with the changes introduced by new technological innovations in the electronic transactions and the system of e-governance.

Chapter -5

Right to privacy and data protection international perspective

CHAPTER -5

Right to Privacy and Data Protection International Perspective

An Overview

The Global technological development and computer related nature of the global economic activities inevitably means that large amount of personal data cross national borders every day, either over communication networks, such as the Internet, or through the manual transfer of media, such as hard disks within notebook computers. Such transfers will predominantly occur in the absence of any form of control or supervision by a regulatory authority. However, such transfer could obviously pose a threat to individual, since national data protection laws may be circumvented by transferring data to a so called 'data haven', which lacks such legislation.

The concept of data protection brings in a paradox which on hand seeks to give an individual a greater measure of control over personal information and to place control over dissemination of information and on the other it conflicts with individual claims to be allowed access to information that may be intrusion in relation to the concept of privacy. The concept of

data protection is one of the most significant contributions to the law of information technology.

International Legal Instruments Protecting Privacy

The Legal protections of the right to privacy in general and of data privacy in particular have various issues around the world and have different directives on data privacy. The basic right to protect an individual's privacy has been enshrined in the Universal Declaration of Human Rights, 1948 (UDHR, 1948)[1]as follows:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and regulation. Everyone has the right to protection of the law against such interference or attacks."

This has also been articulated in various other International covenant and treaties under which privacy is specifically mentioned as a right.

Article 17 of the International Covenant on Civil and Political Rights[2] (ICCPR) provides that (1) No person shall be subject to arbitrary or unlawful interference with his privacy,

[1]Article12; India is a signatory to the UDHR,1948
[2] India is a signatory to the ICCPR, 1966

family, human or correspondence, nor to lawful attacks on his honour and reputation.

(2) Everyone has the right to the protection of the law against such interference or attacks.

Article 16 of the UN Convention on Protection of the Child (UNCPC), Article 14 of the UN Convention on Migrant Workers (UNCMW), Article 8 of the European Convention on Human Rights, Article 11 of the American Convention on Human Rights; all these have set out the right to privacy in terms similar to the UDHR.[3]

The UDHR and the ICCPR are directly binding upon India as it is a signatory to both these international conventions. However, no consequent legislation has been enacted in India to protect the above mentioned rights.[4]

Data Protection Legislations: International Perspective

The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in Germany in 1970; it was the first computer specific statute in

[3] See, http://. Unhcr.ch/huml; Also See, http.conventions.coe.int/Treaty
[4] Aashit Shah and Nilesh Zacharias; 'Right to Privacy and Data Protection'. Nishith Desai Associates, 2001

the form of a Data Protection Act. This statute was widely accepted all over Europe and throughout the world.

This was followed by national laws in Sweden (1973), the United States (1974), again in Germany (1977), in France (1978) and Britain (1984).

A simple distinction between data protection and privacy is made in the 'Lindop Report'[5], When it gives an example that the use of inaccurate or incomplete information, is within the proper scope of data protection, is not necessarily a privacy issue, while data security is a part of the requirements of adequate data protection, it also covers issues of computer systems and computer related crimes.

The parliament of England framed its Data Protection Act (DPA) in the year 1984 which thereafter repealed by the Data Protection Act of 1998. This Act is basically instituted for the purpose of providing protection and privacy of the personal data of the individuals in U.K. The Act covers data which can be used to identify a living person. This includes names, birthday, anniversary dates, addresses, telephone numbers, fax numbers, e-mail addresses etc. It applies only to the data which is held or

[5] Report of the Committee on Data Protection,(Chairman: Sir Norman Lindop) (Cmnd 7341), London; HMSO 1978

intended to be held, on computers or other equipments operating automatically in response to instructions given for that purpose or held in a relevant filing system.

As per the Act, the persons and organizations which store personal data must register with the information commissioner, which has been appointed as the government official to oversee the Act. The Act put restrictions on collection of data. Personal data can be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes. The personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.

Though both U.S. and the European Union focus on enhancing privacy protection of their citizens, U.S takes a different approach to privacy from that of the European Union. US adopted the sectoral approach that relies of mix of legislation, regulation, and self regulation. In U.S, data are grouped into several classes on the basis of their utility and importance. Thereafter, accordingly a different degree of protection is awarded to the different classes of data.

Several Acts were also passed in order to stabilize the data protection laws in the United States. The Privacy Act was

passed in the year 1974 which provided for establishing standards for when it is reasonable, ethical and justifiable for government agencies to compare data in different databases. Another Electronic Communications Privacy Act was passed for restricting the interception of electronic communications and prohibiting the access to stored data without the consent of the user or the communication service.

Further, the Children's Online Privacy Protection Act was passed by the US Congress in October 1998 requiring website operators to obtain parental consent before obtaining personal information from children, and a Consumer Internet Privacy Protection Act required an Internet Service Provider to get permission of the subscriber before disclosing his personal information to third parties.

However, the existing federal laws are not suffice to cover the broad range of issues and circumstances that make the new digital environment a threat to personal privacy. Further, the US Government has been reluctant to impose a regulatory burden on Electronic Commerce activities that could hamper its development and has looked for an answer in self regulation.

Two crucial international instruments evolved from these laws. The Council of Europe's 1981 Convention for the

Protection of Individuals with regard to the Automatic Processing of Personal Data[6] and the Organization for Economic Cooperation and Development (OCED) Guidelines Governing the Protection of Privacy and Trans Border Flows of Personal Data, set out specific rules covering the handling of electronic data. The rules describe personal information as data that are afforded protection at every step from collection to storage and dissemination.

In recent years, in several countries, issues of privacy have been fused with the concept of 'data protection'.

In order to prevent organizations from avoiding data protection controls, and therefore guaranteeing a free flow of information, International governmental organization have themselves involved in attempting to obtain international harmonization for data protection legislation; including the Organization for Economic Cooperation and Development (OCED), United Nations, The Council of Europe, European Union, United States, United Kingdom, Japan, Malaysia, China etc..

[6] http://www.oecd.org/dsti/sti/it/sector/prod/priv-en.htm

The OCED Principles

The Organization for Economic Cooperation and Development (OCED) was established in 1961, and currently comprises 30 leading industrial nations as its member. The nature of the organization has meant that interest in data protection has centered primarily on the promotion of trade and economic advancement of Members States, rather than 'privacy' concerns.

In 1963, a Computer Utilization Group was set up by the third Ministerial Meeting. Aspects of the Group's work concerned with privacy went to a subgroup, the Data Bank Panel. This body issued a set of principles in 1977. In the same year, the working Party of Information Computers and Communications policy [ICCP], was created out of the Computer Utilization and scientific and technical policy groups. Within this body, the Data bank of Panel became the 'Groups of Government Experts on trans border Data Barriers and the Protection of 'Privacy'.

Its remit was to develope guidelines on basic rules governing the Trans border flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation. The OECD guidelines on the protection of

privacy and Trans border Flows of personal Information were drafted in 1979 and adopted in September 1980.[7]The guidelines are based, as with the council of Europe Convention, upon eight, self-explanatory, principles of good data protection practices.

The guidelines are simply recommendations to countries to adopt good data protections practices in order to prevent unnecessary restrictions on Trans border data flows and have no formal authority. However, some companies and trade associations, particularly in the United States and Canada, have formally supported the guidelines.

The **OECD guidelines** consist of **eight basic principles** which are as follows:

1. **Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data Quality Principle**: Personal data should be relevant to the purpose for which they are to be used, and, to the extent

[7] Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Trans border flows of Personal Data, Paris: OCED, 1980.

necessary for those purpose, should be accurate, compete and kept up-to-date.

3. **Purpose Specification Principle**: The purpose for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purpose or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with (Principle 3) except:

(a) With the consent of the data subject; or

(b) By the authority of law.

5. **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risk as loss or unauthorized access, destruction, use modification or disclosure of data.

6. **Openness Principle**. There should be a general policy of openness about developments practices and policies with respect to personal data. Means should be readily available of

establishing existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller.

7. **Individual Participation Principle**: An individual should have the right:-

(a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

(b) To have communicated to him, data relating to him

(i) Within a reasonable time;

(ii) At a charge, if any, that is not excessive;

(iii) In a reasonable manner; and

(iv)In a form that is readily intelligible to him;

(c) To be given reasons if a request made under sub-para is denied and to be able to challenge such denial; and

(d) To challenge data relating to him and; if the challenge is successful, to have the data erased, rectified, completed or amended.

8. **Accountability Principles:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

The OECD guidelines were developed to harmonize national privacy legislations and, at the same time, have much relevance and the directions may be taken by states for privacy protection.

The Council of Europe

The Council of Europe has been the major international force in the area of protection of privacy since 1968. The Council discussed in its forum whether domestic laws gave adequate protection for personal privacy in the light of modern scientific and technical developments and it saw insufficient protection in this area through domestic legislations.

A specialist Committee of Experts on the Protection of Privacy was subsequently asked to draft appropriate resolutions for the Committee of Ministers to adopt. In 1976, a Committee of Experts on Data Protection was constituted to prepare a Convention on the protection of privacy in relation to data processing broad and Trans frontier data processing. In April 1980, the text of the Conventions was finalized, and opened for signature on 28th January 1981.

The Convention came into force of in October 1985 upon ratification by five countries, namely Sweden, Norway, France, Federal Republic of Germany and Spain and in total forty-one members of the Council of Europe has signed the Convention.

The right to data privacy is heavily regulated and rigidly enforced in Europe. Article 8 of the European Convention on Human Rights (ECHR) provides a right to respect for one's *"Private and family life, his home and his correspondence"*, subject to certain restrictions. The European Court of Human Rights has given this Article a very broad interpretation in its jurisprudence. According to the Court's case law the collection of information by officials of the state about an individual without his consent always falls within the scope of Articles of the state about an information for the official census, recording fingerprints and photographs in a policy register, collecting medical data or details of personal expenditures and implementing a system of personal identification have been judged to raise date privacy issues.

Any state interference with a person's privacy is only acceptable for the Court if three conditions are fulfilled.

1. The interference is in accordance with the law
2. The interference pursues a legitimate goal

3. The interference is necessary in a democratic society

The government is not the only entity which may pose a threat to data privacy. Other citizens and private companies most importantly, engage in far more threatening activities, especially since the automated processing of data became widespread. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the European Commission was concerned that diverging data protection legislation would emerge and impede the free flow of data within the EU zone. Therefore the European Commission decided to harmonize data protection regulation and proposed the Directive on the protection of personal data, which member states had to transpose into law the end of 1998.

The directive contains a number of key principles which must be complied with. Anyone processing personal data must comply with the eight enforceable principles of good practice.

They state that the data must:

I. Fairly and lawfully processed.

II. Processed for limited purposes.

III. Adequate, relevant and not excessive.

IV. Accurate.

V. Not kept longer than necessary.

VI. Processed in accordance with the data subject's rights.

VII. Secure.

VIII. Not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controlled towards the individual, although in some limited circumstances exemptions will apply. With processing, definition is far wider than before. For example, it incorporates the concepts of 'obtaining', 'holding' and 'disclosing'.

All EU member states adopted legislation pursuant this directive or adapted their existing law. Each country also has its own supervisory authority to monitor the level of protection.

The council of Europe has been the major international force in the field of data protection since the 1981, 'convention for the protection of Individuals with regard to automatic processing of personal data' was agreed upon.

The majority of the 41 council of Europe members have signed the convention, and have therefore accepted an obligation to incorporate certain data protection principles into national law. The convention came into force of 1 October 1985 when five countries had ratified it: Sweden, Norway, France, Federal Republic of Germany and Spain.

The Council of Europe has been involved in the area since 1968, when the Parliamentary Assembly passed Recommendation 509 [1968], asking the council of Ministers to look at the Human Rights Convention to see if domestic laws gave adequate Protection of personal Privacy in the light of modern scientific and technical developments. The council of Ministers asked the committee of Experts on Human Rights to study the issue, and they reported that quite insufficient protection existed.

A specialist committee of Experts on the protection of privacy was subsequently asked to drafts appropriate resolutions for the committee of Ministers to adopt. Resolutions 22 [1973] covered the 'ground rule' for data protection in the private sector while Resolution 29 [1974] focused on the public sector.

In 1976, the committee of Experts on Data Protection was established. Its primary task was preparing a convention on the

protection of privacy in relations to data processing abroad and Trans frontier data processing. The text of this convention was finalized in April 1980, and opened for signature on 28 January 1981.

The convention is based around a number of basic principle of data protection, upon which each country is expected to draft appropriate legislation. Such legislative provision will provide for a minimum degree of harmonization between signatories, and should therefore prevent restrictions on trans border data flows of reason of 'privacy' protection.

Since 1981, the Committee of Experts on Data Protection has been primarily involved in the drafting of sectoral on rules on data protection. These form part of an ongoing series of recommendations issued by the Committee of Ministers designed to supplement the provision of the convention.

The major weakness of the convention is its lack of enforceability against countries that fail to uphold the basic principles. No enforcement machinery was created under the convention and therefore any disputes have to be resolved at the diplomatic level.

The United Nations

The United Nations has only focused on the human rights aspects of the use of computer technology comparatively recently. In 1989, the United Nations General Assembly (UNGA) adopted a set of drafts guidelines for the regulation of computerized personal data files.[8] These drafts guidelines were subsequently referred to the Commission of Human Right's Special Rapporteur, Mr. Louis Joinet , for redrafting based on the comments and suggestions received from member government and other interested international organizations. A revised version of the guidelines were presented and adopted in 1990.[9] The guidelines are divided into two sections. The first section of these covers 'principle concerning the minimum guarantees that should be provided in the national legislation'. These 'principles' echo these put forward by both the council of Europe Convention and the OECD guidelines, but the UNGA guidelines added three additional terms:

[a] 'principle of non-discrimination'- sensitive data, such as racial or ethnic origin, should not be compiled at all.

---

[8] Resolution 44/132, on 15 December,1989

[9] Adopted by the Commission on Human Rights, Resolution 1990/42 (6 March 1990); subsequently by the UN Economic and Social Council, Resolution 1990/38,14th Plenary Session (25 may 1990), and finally by the UN General Assembly, Resolution 45/95, 68th Plenary Session (14 December 1990).

[b] 'Power to make exceptions'- justified only for reasons of national security, public order, public health and morality.

[c] 'Supervision and sanctions'- the data protection authority 'shall offer guarantees of impartiality, independence vis-a-vis person of agencies responsible for processing and technical competence. [10]

The second sections consider the 'applications of the guidelines to personal data files kept by governmental international organization'. This requires that international organization designate a particular supervisory authority to oversee their compliance. In addition, it includes a 'humanitarian clause', which states that: A derogation from these principles may be specifically provided for when the purpose of the file is the protections of human rights and fundamental freedom of individual concerned or humanitarian assistance.

Such a clause is intended to cover such organization as Amnesty International, who hold large amounts of personal data, but would be wary of sending of information out to a data

[10] Ian Walden, "Data Protection", in Chris Reed & John Angel (eds.), Computer Law,447-448 (4th ed., 2002)

subjects on the basis of an access request made while the person was still imprisoned.

The European Union

Despite interest and involvement in data protection and privacy issue for nearly two decades, from both the European Parliament and the commission, the emergence of a directive connecting this area only appeared in 1990. The European parliament's involvement in data protection issues has primarily been through its Legal Affairs Committee, though the issue has been subject to parliamentary question and debates for the past 10 years.

In 1976, the European parliament's adopted a resolution calling for a directive to ensure that 'Community citizens enjoy maximum protection against abuses of failures of data processing' as well as 'to avoid the development of conflicting legislation'.[11]In 1977 the Legal Affairs Committee established the Subcommittee on Data Processing and the Rights of the

[11] Resolution on the protection of the rights of individuals in constitution with data processing; oj c100, 3may 1976, p.27

individual. The Sub committee, produced the 'Bayerl Reports' in May 1979.[12]

The result debate in the European Parliament led or recommendations being made to the Commission and the council of Ministers concerning the Principles that should form the basis of community's attitude to data protections.[13] These recommendations called on the European commission to draft a directive to complement a common communications system, to harmonize the data protection laws and secure the privacy of Information on Individual in computer files. In July 1981, the European commission recommended that all Members should sign the council of Europe convention and seek to ratify it by the end of 1982.[14]

A second parliament report, the 'Sieglerschidt' Report, was published in 1982.[15] The report noted 'that data transmission in general should be placed on a legal footing and not to be determined merely by technical reason'. It recommended to the establishment of a 'European Zone', of

[12] Report on the protection of the individual in the face of the technical developments in data processing, 1979-1980 EUR. Parl.Doc. (no 100) 13 (1979)
[13] OJ C140, 5 June 1979,P.34
[14] commission recommendation of 29 July 1981, relating to the Council of Europe convention for the protection of individuals with regard to automatic processing of personal data, ojl247/31, 29 August 1979, 81/679/EC
[15] second report on the protection of the right of the individual in the face of technical development in data processing,e.p.doc.1-548/81,12 October 1981

members in the ECC and Council of Europe, within each authorization prior to the export of data would not be needed. It also indicated that initiatives, such as a Directive, were still necessary, following the report, a resolution was adopted by the European Parliament, on 9 March 1982, calling for a directive if the convention proved inadequate.

In July 1990, the European Commission finally published a proposed Directive on data protection. It was published as part of a package of proposal, which included a recommendation that the European Community adheres to the Council of Europe Convention on data protection,[16] a declaration applying data protection principles to Community institutions,[17]a draft directive addressing data protection issues in the telecommunications sector,[18] and a draft council decision to adopt a two-year plan in the area of security for information systems.[19] After considerable controversy and political debate at

[16] However, See the European court of justice opinion no-2/94 (1996) 2 cmlr 265 that the community cannot adhere to the European convention on human rights.

[17] commission declaration on the application to the institution and other bodies of the European communities of the principles contained in the council directive concerning the protection of individuals in relation to the processing of personal data (com (90) 314 final, ojc277/74,5 November 1990.

[18] Finally adopted in 1997; directive 97/66/EC of the European parliament and of the council concerning the processing of personal data and the protection of privacy in the telecommunication sector, ojl24, 30 January 1998. Implemented in the United Kingdom by the telecommunication (data protection and privacy) regulations 1999, si 1999/ 2093.

[19] Adopted as council decision 92/242/EC of 31 March 1992, in the field of

all stages of the legislative process, the general framework Directive on data protection was finally adopted by the European Parliament and council on 24 October 1995.[20] Members states had to implement the directive by 24 October 1998, although only five managed to adopt legislation by that date.[21]

The provision of the directive shall be considered below in the context of the United Kingdom's implementing stature: the Data Protection Act 1998. The primary justification for a commission action was a part of the Single Market Programme, under Art. 100 (a) of the E U Treaty.

In 1990 only eight of the (then) twelve Members states have passed data protection legislation. Even between these eight considerable divergences existed in terms of scope of protection; the nature of the obligations imposed on data user and the restrictions on use and export of data. Such differences were seen as a potential obstacle to the development of integrated European Information Market.

---

information security, ojl123, 8May 1992.

[20] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, ojl 281, 23 November 1995.

[21] Greece, Italy, Portugal, Sweden, and the United Kingdom (UK), although the UK had not implemented the legislation.

The Commission also expressed its desire to protects the right of individual data subject, 'and in particular their right to privacy' (Art. 1(1)).

The directive is therefore limited to the protection of natural person, rather than legal person. [22]

United States of America

"Perhaps the most salient characteristic of legal protection of information privacy in the united states is its *ad hoc nature*, some types of information transfers are heavily regulated, while other types, seemingly no less significant to individual privacy interests, are unregulated and left to the mercies of the marketplace."[23]

The issue of privacy in the area of communication started to develop in the US Legislations since the late 1960s. In 1968, the US congress enacted the omnibus crime control and safe streets act, primarily focused on telephone wiretaps. Later, it was broadened to include digital electronic communication.[24] The Electronic Communication Privacy Act, 1968 (ECPA) in

[22] However, the telecommunications data protection directive does confer certain rights upon 'subscribers', who may be natural or legal persons (Art.2 (a)).
[23] Margaret Jane Radin, "Privacy Online, in Internet Commerce: The Emerging Legal Framework" 548. (Foundation Press, New York, 2002)
[24] Vakul Sharma, Handbook of Cyber Law 93 (1st Ed., Macmillan India Ltd., 2002).

the US makes it illegal to intercept or disclose private communications and provide victims of such conduct, a right to sue anyone violating his mandate.

Under the ECPA, violation of privacy of electronic communication means an intentional interception of any electronic communications or its international use or disclosure.[25]

The Fourth, Fifth and Ninth amendments to the US Constitution addressed the issue of privacy, though not expressly, but just like Indian constitution in an implied manner.

At the same time, several legislations were enabled dealing with the online environment. Some of these Legislations are, the Fair Credit Reporting Act, 1970, the Family Education Rights and Privacy Act, 1974, the Driver's Privacy Protection, 1974, the Fair Debt Collection Practices Act, the Right to Financial Privacy Act, 1978, the Cable Communications Policy act, 1984, the Privacy Protection Act, 1980, the Computer Fraud and Abuse Act, 1986, the Telephone Consumer Protection Act, 1991, the Privacy Act, 1994 and the National Information Infrastructure Protection Act, 1996.

[25] Ian Walden, "Data Protection", in Chris Reed & John Angel (eds.), Computer Law,451-453 (4th ed., 2002)

The Federal Trade Commission (FTC) in the USA has been playing an important role in the development of a federal legal system towards the issue of information privacy. In June 1998, the FTC submitted a report to the congress, on which basis Online Privacy Protection Act came into effect from April 2000. Now, intrusion into the privacy of children is allowed only after obtaining consent of parents.

The US senate judiciary committee approved hacker's bill in October 2001. It clarifies federal law enforcement authority's power to prosecute hackers. The US federal laws basically protect the privacy of financial information transmitted via telecommunications system, and in recent years, its laws deal with the online privacy.

United Kingdom

In recent years, in the U.K., several steps have been taken with regarded to Data protection. But way back in 1961, Lord Mancroft introduced a right of privacy bill, this bill marked the beginning of a 23-year history which finally led to the successful passage of data protection act 1984. In May 1970, a committee on privacy was appointed under the chairmanship of Kenneth Younger. The Younger report was completed and presented to the Parliament in July 1972.

In response to the Younger report, the government promised a white paper. However, it was three years before the white paper on Computers and Privacy (cmnd6353) was presented to Parliament in December 1975. In it the government accepted the need for legislation to protect computer-based information. The government felt that computers posed a special threat to individual privacy.

The government also issued a second white paper, entitled computers: safeguards for privacy (cmnd6354), which agreed with the comments made by the Younger report. The creation of a data protection authority was also proposed to supervise the legislation and ensure that appropriate safeguards for individual privacy were implemented. The government came with a third white paper (cmnd 8539) in 1982 and the Data Protection Act of 1984 received royal assent on 12 July 1984. The Act became operational on 11 November 1987. To comply with its obligations to implement EU directive 95/46/EC, the U. K. came out with the Data Protection Act, 1998, which received royal assent on 16 July 1998.

The Data Protection Act, 1998 is concerned with personal data. 'Personal data' consists of data that relates to a 'living individual' who can be identified from that data, or information

in the possession of the data user. 'Data' includes information processed by computers, 'relevant filing system' and 'accessible records'.

This legislation was backed up by several court decisions and the U. K. government has entered the world of cyber regulation with comprehensive guidelines.

The trade and industry regulations allow the bosses' access to staff calls, e-mails and internet activities without the employee's knowledge for a wide variety of reasons. Routine access to business communications in the regulations includes monitoring standards of service and training, combating crime and unauthorized use of company system. It has been welcomed as a 'legitimate business need' by the industries but it is the lack of consent and the vagueness of 'unauthorized usage' that have civil liberties groups and unions up in arms. They argue that these rules conflict with two things, a recent data protection commission code on surveillance, which emphasizes consent, and the guarantee in the new Human Rights Act, 1998 according to which everyone has the right to privacy for correspondence.

Other countries such as Germany depend more on a workplace consensus and Scandinavian countries demand consent before undertaking electronic surveillance.[26]

Japan

The Japanese Constitution enshrines freedom of speech, assembly and association. The 1988 Act for the Protection of Computer Processed Personal Data held by administrative organs and 1990 Protection of Computer Processed Personal Data (based on the OECD guidelines) provide partial regulation for national government agencies vis-à-vis data protection and privacy.

The national government has emphasized self- regulation by the private sector, especially regarding privacy aspect of electronic commerce, with a series of inspirational guidelines from the ministry of international trade & industry (MITI) and other agencies.

The Personal Data Protection Act, passed in May 2003, has established some general restrictions on the use and sharing of personal data, also giving individuals the right to obtain information collected by some private sector bodies.

[26] Deepti Chopra and Keith Merrill, "Cyber Cops, Cyber Criminals and Internet" 287-88 I.K. International Ltd., New Delhi, 2002

Malaysia

Malaysia also proposed a Personal Data Protection Act recently in 2003. It breaks new ground in law making for cyber-privacy. According to the Malaysian government, the legislation is envisaged to be a world-class leading edge cyber law that provides for higher level of personal data protection. This Act seeks to -

(a) provide adequate security and privacy in handling personal information;
(b) create confidence among consumers and user of both networked and non networked industries;
(c) accelerate uptake of e- commerce; and
(d) promote a secured electronic environment in line with multimedia super corridor (MSC) objectives.

The rationale, the government said, is to promote Malaysia as a communization and multimedia hub where the national adoption of e-based transactions is expected to be high.

China

The China's Internet law as well as the related information technology legal infrastructure as a whole is still not well

developed. However, the China has got various types of measures to the protection of privacy.[27]

Constitutional Protection to Privacy in China

Article 38 of Constitution provides that human dignity of citizens should not be infringed. Article 39 provides that the premises should not be trespassed. Article 40 stipulates that the freedom and privacy of correspondence of citizens are protected by law. These are the parts of the privacy of citizens and general principles set out by the Constitution as the basic law. Moreover, these provisions may provide the basis for the protection of privacy by other laws and regulations.

Civil Law in China & Protection to Privacy

In Civil Law, there are no explicit provisions identifying the right of privacy as the right of personality of citizens in the General Principles of Civil Law, 1986.

The opinions of the Supreme People's Court of China on several issues, concerning the implementation of the General Principles of Civil Law of the People's Republic of China does not treat the right of privacy as a separate right of personality. It only stipulates that in case anyone propagates the privacy of any

[27] See, Internet Business Law Services, Inc. (2001-2008)

other person in writing or orally, which result in certain influence, such act should be determined as an act infringing the citizen's right of reputation.

Criminal Law in China & Protection to Privacy

Anyone who intentionally infringes the privacy of others, causing serious consequences, should be subject to criminal penalties.

The Criminal Law of China provides that whoever conceals destroys or unlawfully opens another person's letter thereby infringing upon the citizen's right to freedom of correspondence, if the circumstances are serious, shall be sentenced to fixed term imprisonment of not more than one year of criminal detention.[28]

The Criminal Law of China also provides that any postal worker who opens without authorization or conceals or destroys mail or telegrams shall be sentenced to fixed term imprisonment of not more than two years of criminal detention.[29]

The infringement is not convicted of the crime of invasion of privacy, but the crime of violation of freedom of

[28] Article 252
[29] Article 253

communication and the crime of opening, concealing and destroying mails and telegrams.

Internet and Legal Protection to Privacy in China

In China, the provisions on the Technical Measures the Protection of the Security of the Internet were promulgated by the Ministry of Public Security on March 1, 2006. It requires that the provider of the Internet services and entity users of the network should be responsible for carrying into effect the technical measures for the protection of the Internet security and should guarantee normal functioning of the technical measures for the protection of the Internet security.

The providers of the Internet services and entity users of the network should establish corresponding administration system. The information as registered by users should not be publicized or divulged without the approval of the users unless it is provided for by any law or regulation.

The Measures for Security Protection Administration of the International Networking of Computer Information Networks in People's Republic of China provides that user's freedom of communication and communication secrecy are

provided by law.[30] No unit or individual shall use the international networking to infringe on user's freedom of communication and communication secrecy in violation of the provisions of law.

Article 18 of the Implementations Rules for Provisional Regulations of the Administration of the International Networking of Computer Information in the People's Republic of China provides that it is prohibited to infringe on the privacy of others by accessing computer systems without authorization, tampering with the information of others or sending information in the name of others.

The review of International instruments and practices addressing data protection and privacy issues reveals that the issue of data protection related to distinct areas such as privacy and data security needed a distinct legislative ventures which can be analyzed and formulated by one of the most acceptable definitions of 'data protection' is given in the British Government's report, appended to the draft of the Council of Europe Convention on Data protection, the legal protection of

[30] Article 7

individuals with regard to automatic processing of personal information relating to them.[31]

Another view on data protection legislation provides 'data protection' as 'fairness legislation' not requiring a balance between data users and data subjects, but simply being fair to an individual.[32] In theoretical perspective, Data protections law as a distinctive legislative field is predominantly a European phenomenon. Currently such law exists in some 25 European countries.[33]

Outside Europe other countries e.g. Australia, Japan & Canada have also adopted the data protection regime but in some different approach to European Models of data protections laws. These countries have emphasized data protection laws to public Sector data processing activities, not the private sector.

Some European Nations, such as Denmark, Austria & Italy extended the protection afforded under data protections

---

[31] Convention for the Protection of Individuals with regard to 'Automatic Processing of Personal Data' , Strasbourg ,28 January (cmnd 8341),London : HMSO,1981 : Explanatory Report p.5

[32] CBI, Conference, London, 4 March 1988.

[33] *AUSTRIA, BELGIUM, CZECH AND SLOVAK REPUBLICS, DENMARK, FINLAND, FRANCE, GERMANY, GREECE, GUERNSEY, HUNGRY, ICELAND, IRELAND, ISLE OF MAN, ITALY , JERSEY, LUXEMBOERG,THE NETHERLANDS, NORWAY, POLAND, PORTUGAL, SPAIN, SWEDEN, SWITZERLAND AND THE U.K.*

laws to legal persons, such as companies, trade unions as well as individuals.

In other Nations of Europe, like France and the Netherlands, data protection laws have always applied to mammal records, as well as computer data within Europe, the 1981 council of Europe convention on data protection has been the foundation upon which national legislations and the 1995 European Union direction has been constructed.

Two distinct motives underline the 1981 convention.[34]

1. The threat to individual privacy posed by computerization and interrelated technological developments.
2. The desire to maintain a free flow information amongst the countries in relation to automatic processing of data which is better known as trans border data flows.

Therefore, the convention attempts to reconcile Article 8 of the European Human Rights Convention, concerning an individual's right to privacy, with the principle of free flow of information, enshrined in Article 10 of the Human Rights convention protecting freedom of expression.

---

[34] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January (cmnd 8341),London : HMSO,1981 : Explanatory Report p.5

In this age of Information technology and the use of Internet, the adoption and enforcement of data protection by means of self-regulatory measures [35]may not be complete solution regarding the international flow of data.

However, the promotion of general principles of good information practices, together with an international and independent supervisory regime, may enable the law to maintain sufficient flexibility to achieve balance between the need to protect the rights of individuals and to control how data about them is used, and the specific needs of networked global economy with the adoption of e-transactions in this era of information technology.

[35] See the 'Safe-Harbor' initiative issued by the US Department of Commerce (November 1999).

Chapter-6

Right to privacy and data privacy the remedial perspectives

CHAPTER-6

Right to Privacy and Data Privacy
The Remedial Perspectives

An Overview

The legal and regulatory issues indicate that the challenges posed by the Information Technology are not easy to be resolved merely by adopting and extending the existing legal concepts. The infrastructure of Information Communication Technologies i.e. telecommunication technologies and the Internet, even if global in scope is not an absolutist free domain, but it is subject to innumerable national and International restrictions in the form of regulatory laws.

At the same time, the very infrastructural support of the convergence in technologies in substance diminishes the chances for enforcement of national laws of control and regulations in terms of limited jurisdiction.

The e-transactions and lack of regulatory mechanisms for state legislations and national borders is making a great impact on the issue of privacy protection in general. Attempts to erect

infrastructural support and national barriers against subversive or culturally polluting information are readily circumvented.[1]

National laws restriction can be enforced directly only within the territory (jurisdiction) to which they apply. But the global reach of Internet for the flow of information may easily transfer and may effectively break the barriers of privacy.

Information sources need not necessarily to be disseminated by giving a serious and certified mechanism to fix the liability, which is better known as *service provider's liability*. Therefore, the ease of digitization of data and sharing it across in global networks means that our personal information may not be so private anymore, which poses unforeseen risks.

Nowadays, most of the valuable information stored with corporations is vulnerable to theft (hacking). Moreover, even governments, with the best data protection tools at their disposal have been known to lose medical and financial information for millions of people. In year 2007, the United Kingdom Government lost the personal records of over 25 million tax

[1] See 'On-Line Boundaries: Internet Tramples Legal Jurisdiction' (1995) Computer World, June 5, New Delhi, P 1.

payers, the most high profile example of such information getting lost.[2]

Privacy Regulation Models

The privacy of individuals is certainly a challenge because information can be generated indirectly at very low cost and as a consequence this personal information can be used commercially.

Taking this to legal and policy response, the following approaches as existing in various legal systems may be useful to meet out with privacy concerns:

- Home Country Regulation
- Self Regulation
- Legislation
- Reliance on Third Parties for Enforcement of International Standards

The integrated approach of above mentioned measures may be helpful to protect the privacy and online data.

[2] The Times of India, New Delhi, August 05, 2008, "Keep it private".

The Remedial Perspectives of Privacy and Data Protection

The UK has a much more legislative approach to the protection of personal data in general as compared to the U. S. Data Protection Act, 1998 came into force recently, on the March 1, 2000. It lays down rules for processing personal information and applies to paper records as well as those held on computers.

The rules provide that anyone processing personal data must comply with the eight enforceable principles of practice.

That data must be-

- fairly and lawfully processed;
- processed for limited purpose;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's right;
- secure;
- not transferred to countries without adequate protection.[3]

[3] This is an interesting provision, similar to many others present in other European countries. It would be interesting to know whether the U. S.A. would fall under this category.

The Legislative Responses in U.K. and European Union

In 1961, Lord Mancroft Introduced a *'Right of Privacy'* Bill. This Bill can be seen to mark the beginning of a 23 year history which finally led to the successful passage of the Date Protection Act 1984. This first private member's Bill was followed by four others until the government finally decided to establish a formal committee of inquiry into this area.

In May 1970, a Committee on Privacy was appointed under the Chairmanship of Kenneth Younger (the Younger Report).The committee's purview was limited to the private sector despite the Committee' request that it may be reviewed. The final report was completed and presented to Parliament in July 1972.[4]

During its establishment, the Committee set up a special Working Party on Computers. The working Party (at Para. 580) concluded that put quite simply, the computer problem as it affects privacy in Great Britain is one of apprehensions and fears and not so far one of facts and figures.

Indeed, their report went on to note that the most credible anxieties were those held about computers in the public sector,

[4] Report of the Committee on Privacy (Cmnd 5012), London HMSO, 1972.

an area outside the Committee's scope. The Committee noted that the main areas of public concern were with universities, bank records and credit agencies. The Committee recommended that an independent body (standing commission) composed of computer experts and lay persons should be established to monitor growth in the processing of personal information by computer, as well as the use of new technologies and practices.

In response to the Younger Report, the government promised a White Paper. However, it was three years before the White Paper, *Computers and Privacy* (Cmnd6353) was presented to Parliament in December 1975. In it, the government accepted the need for legislation to protect computer-based information. Despite the concerns expressed in the Younger Report with regard to manual records, the government felt that computer posed a special threat to individual privacy.

The speed of computers, their capacity to store, combine, retrieve and transfer date, their flexibility, and the low unit cost of the work which they can do have the following practical implications for privacy:

(1) They facilitate the maintenance of extensive record systems and the retention of data on those systems;

(2) They can make data easily and quickly accessible from many distant points;

(3) They make it possible for data to be transferred quickly from one information system to another;

(4) They make it possible for data to be combined in ways which might not otherwise be practicable;

(5) Because the data are stored, processed and often transmitted in a form which is not directly intelligible, few people may know what is in the records, or what is happening to them.

The government also issued a second White Paper, entitled *Computers: Safeguards for Privacy* (Cmnd 6354), which agreed with the comments made by the Younger Report with regard to the concerns generated by public sector information.

Rather than to establish a standing commission to monitor the use of personal date, the White Paper proposed legislation to cover both public and private sector information systems. The creation of a Data Protection Authority was also proposed to supervise the legislation and ensure that appropriate safeguards for individual privacy were implemented. In order to provide a

detailed structure for the proposed data protection authority, the government established a Data Protection Committee, under the chairmanship of Sir Norman Lindop, which reported in 1978.

The *'Lindop Report'* proposed that a number of data protection principles should form the core of the legislation, with the Data Protection Authority being responsible for ensuring compliance with those principles. In particular, the Authority would be required to draft codes of practice for various sectors based on consultations with interested parties and associations, which would then become law, as statutory instruments. Failure to comply with a code would lead to criminal sanctions. Overall, the *'Lindop Report'* was concerned to produce a flexible solution which would not act so as to hold back the growing use of the government in 1979, legislation on data protection was further delayed. Finally, in 1982, the government issued the White Paper on Data Protection, the Government's proposals for Legislation (Cmnd 8539). The approach put forward in the White Paper was much less thorough than that proposed in the Lindop Report, the idea of a Data Protection Law. The White Paper also rejected the idea of statutory codes of practice. Although they saw the value of such codes, the government felt that the length of time necessary to

create an adequate range of statutory codes of practice would be unacceptable.

The Data Protection Act of 1984 received the Royal Assent on 12 July 1984. The provisions of the Act were phased in over a three-year period, with the Act becoming fully operational on 11 November 1987.

Further, the Data Protection Act 1998 received Royal Assent on 16 July 1998. The Act enables the government to comply with its obligation to implement EU Directive *95/46/EC*. It repeals the 1984 Act, although transitional provisions in the 1998 Act effectively mean that processing carried out prior to 24 October 1998 will continue to be subject to the 1984 Act until October 2001. The 1998 Act did not enter into force until 1 March 2000, when the necessary ministerial orders under the Act had been drafted.[5]

The following sections primarily consider the provisions of the 1998 Act, although some of the detailed procedural aspects have yet to be finalized. However, reference will also be made to the 1984 Act, since much of the case law that has arisen

[5] See, S. Chalton, S. Gaskin, H. Grant & I. Walden (eds); Encyclopedia of Data Protection, Sweet & Maxwell , London

under the Act will continue to be applicable when considering how such legislation impacts on the processing of personal data.

The Data Protection Act 1998 is concerned with personal data. 'Personal data' consists of data that related to a 'living individual' who can be identified from that data, or from that and other data or information in the possession of the data user. 'Data' includes information processed by computers, 'relevant filing systems' and 'accessible records'.[6]

Information must be 'structured, either by reference to individuals or by reference to criteria relating to individual is readily available' (s.1).

The term 'accessible records' has been incorporated in order that the UK government can comply with the European Court of Human Right's decision in *Gaskin v United Kingdom,*[7] In this case, the Court held that certain records related to 'private and family life' in such a way that the issue of access falls within the ambit of Article 8 of the European Convention on Human Rights (ECHR). The government has defined the types of records which it believes fall within the scope of the

[6] Under the government's proposed freedom of Information Bill, the definition will be further extended to include information recorded by a public authority (clause 60).
[7] (1989) 12 EHRR 36

Gaskin decision, including health and educational records (S. 68 and sch. 12).

Under the 1984 Act, the processing of personal data is limited to processing 'by reference to the data subject'.[8] Such a limitation is not present in the 1998 Act's definition of processing which follows the all-encompassing definition in Directive *95/46/EC.*

The 1998 Act is primarily concerned with *three* categories of persons:

(a) '*Data subjects*'- the individual which is the subject of the personal data.

(b) '*Data controllers*'- a person who, whether alone, jointly or in common with others, 'determines the purposes for which and the manner in which' the data are processed.[9]

[8] See, *Equifax Europe Ltd v Data Protection Registrar* (1991) Case DA/90 25/49/7, where the Data Protection Tribunal held that the phrase 'processing by reference to data subject' meant that 'the object of the exercise is to learn something about individuals'.

[9] In *Data Protection Registrar v Francis Joseph Griffin* (QB, 22 February 1993), The Times, 5 March 1993, the court held that limitations imposed on an individual's use of personal data for his own purposes, either contractual or professional, does not necessarily prevent him from being a separate registerable 'data user' under the 1984 Act.

(c) '*Data processor*'- a third party simply processes personal data on behalf of a data controller without controlling the contents of use of the data.

Under the regime established by the EU Directive *95/46/EC*, a key concept is that of 'data subject's consent'. If the data controller obtains consent then he is able to process the personal data. The Directive defines 'data subject's consent' as being freely given, specific and informed. It supplements this in the substantive provisions when referring to consent as being 'unambiguously given'. Such terminology seems to provide little opportunity for a data controller to rely on the implied consent of the data subject. Significantly, however, the 1998 Act does not include any definition of 'consent'. In justification of this position, the Government has stated:

"The Government is content for the issue of whether consent has been validly given to be determined by the court in the normal way. It is better for the courts to decide according to ordinary principles of law than for the Act to contain specific consent provisions."[10]

[10] Comments made by Mr. Hoon (Parliamentary Secretary, Lord Chancellor's Department). 12th sitting of Standing Committee D, 04 June 1998 (Morning).

However, this absence may provide data controllers with greater flexibility with respect to claiming the consent of the data subject through implication, although the courts would have to consider the terminology used in the Directive when interpreting the application of the Act.

Provisions concerning so-called 'sensitive data' were contained in the 1984 Act, but were never brought into operation by the Secretary of State.[11]

Under the new Act, Section 2 defines eight categories of 'sensitive personal data', including data concerning a person's racial or ethnic origin; their political and religious beliefs; trade union membership; physical and mental health and criminal convictions. The processing of sensitive data is subject to additional controls.[12]

Data Protection Principles

The Data Protection Act 1984 was built around certain data protection principles, and the EU Directive *95/46/EC* and the Data Protection Act, 1998 reiterate this approach. These principles are intended to be good practices that data controllers

[11] Data Protection Act 1984, S. 2(3).
[12] See, The Data Protection Act 1998, sch. 3 and The Data Protection (Processing of Sensitive Personal Data) Order 1999 (SI 417/2000).

should comply with in order to protect the data they hold, in both their interests and those of their data subjects.

These principles are fundamental to an understanding of the basis of data protection law in Europe. The 1998 Act contains a limited redraft and renumbering of the 1984 principles, and data controllers have a duty to comply with the principles, except where an exemption exists S.4(4).

The *first principle* requires fair and lawful processing, with the additional requirement that one of the conditions in sch. 2 (and sch. 3 where sensitive data is processed) are present. These conditions primarily relate to the issue of lawful processing. Schedules 2 and 3 therefore substantially extend the concept of 'lawful' processing under the 1984 Act.

The basic position under schs 2 and 3 is that, except where the data controller has the consent of the data subject, the processing of personal data must be 'necessary' for the stated purposes, such as 'the performance of contract to which the data subject is a party'. The burden will be upon the data controller to show evidence of such necessity.

Under the EU Directive, a data controller is required to provide certain information to the data subject, either when the

data are collected from the data subject (Art. 10), or where the data were not obtained from the data subject (Art. 11). These provisions have been incorporated into the Act within 'lawful' processing , this constitutes a significant extension to the interpretation of 'fairness' under the 1984 Act.

In *Innovation (Mail Order) Ltd v Data Protection Registrar*[13], the Data Protection Tribunal stated that fair obtaining' means that at the time that information is collected, the data user needs to inform the data subject of certain matters that will enable the individual to decide whether to provide the information or not. In particular, this includes information about the intended uses for the data, unless such use could be considered obvious.

Whilst the Directive refers only to the data controller providing such information to the data subject, 'except where he already has it', the Act also enables the data controller to comply with the obligation by making the information 'readily available' to the data subject. The manner in which this phrase is interpreted may have important implications for a controller in terms of the procedural mechanisms it establishes, such as the

[13] (29 Sept. 1993; Case DA/92 31/49/1)

use of intranet-based techniques to disseminate information to employees.

Where the data controller has not obtained the data from the data subject themselves, the controller is exempted from the requirement to provide information where it would involve either 'disproportionate effort', or the recording or disclosure is required under a non-contractual legal obligation.[14]

Under the *second principle*, data controllers must obtain data only for specified and lawful purposes, and must not carry out any further processing which is incompatible with those purposes. For Example, a contravention of this principle would be for an organization to register the holding of personal data for purposes of personnel management and use it additionally for marketing purpose.

The *third principle* requires a data controller to only hold personal data that is 'adequate, relevant and not excessive in relation to the purpose or those purposes'.

The *fourth principle* requires that all personal data 'shall be accurate and, where necessary, kept up to date'. If, for example, an organization purports to keep a list of undischarged

[14] See, The Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 1999 (SI 185/2000).

bankrupts, but makes no effort to seek information on persons discharging themselves from bankruptcy, it will be contravening this principle.

The *fifth principle* states that personal data 'shall not be kept for longer than is necessary for that purpose or those purposes'. This principle implies that data should be destroyed when the specified purpose(s) for which they were collected has been achieved.

The *sixth principle* requires processing to be carried out in accordance with the rights of data subjects under the Act.

The *seventh principle* addresses issues of data security, requiring data controllers to take 'appropriate technical and organizational measures' against unauthorized or unlawful processing, and accidental loss, destruction or damage to the data. Regard must be had to the state of technological development and the cost of implementing such measures. Data controllers should also take measures to ensure that employees are reliable and, if using a data processor, contractual obligations must be provided for to ensure that the processor implements security measures.

The obligation upon data controllers not to transfer personal data to countries which do not have and 'adequate' level of protection, as required by the Directive's under Art. 25, is implemented in the Act through a new eighth principle.

Personal data shall not be transferred to a country or territory outside the *European Economic Area(EEA)* unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Principle is accompanied by an interpretation section (sch. 1, pt. II) and by sch. 4, which details situations where the principle is not applicable.

Data controllers will also be required to notify the Commissioner of those countries outside the European Economic Area to which thy transfer, or intend to transfer, personal data. This will enable her to take proactive steps against transfers to countries perceived as providing inadequate protection.

The *eighth principle* will require an assessment of 'adequacy' on a country-by-country basis.

In procedural terms, where a data controller intends to transfer personal data, the first issue that will need to be addressed is whether the transfer falls within one of the criteria specified in sch. 4. If it does, then the eighth principle would not be applicable.

Schedule 4 substantially echoes the derogations provided for under Art. 26 (1) of the Directive. Article 26(2) provides an additional circumstance arising where a Member State, through the offices of the Data Protection Commissioner, authorizes 'a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection'. Such authorizations will only arise where the data controller 'adduces adequate safeguards'. The initiative is clearly upon the individual data controller to seek such authorization before making a transfer.

Under the Act, the Directive's of Art. 26(2) have been implemented through two distinct procedural situations:

(a) The transfer 'is made on terms of a kind approved by the Commissioner'; or

(b) The transfer 'has been authorized by the Commissioner'.

The former is addressed to the possibility that the Commissioner could approve the use of certain contractual terms, which would then be considered suitable to cover a 'set of transfers' carried out by the data controller over a period of time (see section 13.3.5). The latter procedure seems to presume some form of case-by-case prior authorization process.

The Commissioner is required to notify the European Commission and the other Member States of all approvals and authorizations granted. Objections may be lodged against such decisions and the European Commission, through its Committee procedure under Art. 31 may make a determination prohibiting such an authorization. Therefore, any approval or authorization a data controller obtains from the Commissioner must be viewed as qualified, subject to this consultations process.

Where a transfer does fall within the scope of the eight principle, then a data controller will need to assess whether the 'country or territory' to which the interpretation provision, pt. II of sch. 1, provides a non-exclusive list of criteria relevant to the making of such an assessment, echoing the terminology of Art. 25(2) of particular interest is Para. 13(g), which states: Any relevant codes of conduct or other rules which are enforceable

in that country or territory whether generally or by arrangement in particular cases.

This is phrased in broad enough terms to include contractual mechanisms, as rules may be 'enforceable' through contractual agreement. Such an interpretation suggests that contractual mechanisms governing trans border data flows will be a factor both in cases where the eighth principle applies and where it does not. The advantage of the former approach is avoidance of the notification procedure.[15]

The U.S. Position

The Federal Trade Commission (FTC) has played a key role in the development of the response of the US federal legal system to the issue of information privacy. In 1998, it brought out a report, namely-

Privacy Online: A Report to Congress, which was the result of a three tier privacy initiative.

The report recognized four core principles of fair information practice:

- Consumers must be given notice of an entity's

[15] See Generally, Guidance Note, 'The Eighth Data Protection Principle and Trans Border Data Flows' (July 1999, Version 1).

information practices; (The Notice/ Awareness Principle)

- They must have a choice with respect to the use and dissemination of information; (The Choice/ Consent Principle)
- They should have access to any information collected about them; (The Access/Participation Principle)and,
- Finally, consumers must have sufficient security. from the data collector. (The Security/Integrity Principle)

It was acknowledged that these principles are essential to ensure the information privacy interests are adequately protected.

U.S. DEPARTMENT OF COMMERCE, SAFE HARBOR PRINCIPLES, NOVEMBER 1999

The 'Safe Harbor' system allows personal data to be transferred under certain principles.[16] U.S. companies have been able to sign up for it from 1 November 2000 and the EU member states are also supposed to take all the measures necessary to comply with the safe harbor.

The substance of safe harbor consists of seven data processing principles in the areas of notice, choice, onward

[16] Full Documentation concerning safe harbor, including a list of companies belonging to it, available at http//www.export.gov/safeharbor/sh_overview.html.

transfer, security, data integrity, access, and enforcement to be complied with in relation to data received.

Notice: An organization must inform individuals about the purposes of which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the type of third parties to which it discloses the information, and the choices and means the organizations is using or disclosing it for a purpose other than that for which it was originally collected or for a purpose which it was processed by the transferring organization. This notice must be provided in clear and conspicuous language when individuals are fist asked to provide personal information to the organization or as soon as is practicable, but in any event before the organization uses or discloses such information for a purpose other than that specified above.

Choice: An organization must offer individuals the opportunity to choose (opt out) whether and how personal information the provide is used disclosed to third parties, where such use or disclosure is incompatible with the purposes(s) for which it was originally collected or subsequently authorized by the individual.

For sensitive information, (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual) they must be given affirmative or explicit (opt in) choice if the information is to be used for a purpose other than those for which it was originally collected or disclosed to any type of third party other than those already notified to the individual, or used or disclosed in a manner other than as subsequently authorized by the individual through the exercise of opt in choice. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

Onward Transfer: An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice (because a use is not incompatible with a purpose for which the data was originally collected or which was subsequently authorized by the individual) and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring

that the third party provides at least the same level of privacy protection as is required by the relevant principles. If the organization complies with these requirements, it shall not be held responsible when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations.

Security: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data Integrity: Consistent with the principles, an organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for that purpose, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the

case in question, or where the rights of persons other than the individual would be violated.

Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include:

(a) Readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the principles and damages awarded where the applicable law or private sector initiatives so provide;

(b) Follow up procedures for verifying that the attestations and assertions business make about their privacy practices are true and that privacy practices have been implemented as presented; and

(c) Obligations to remedy problems arising out of failure to comply with the principles by organizations announcing their adherence to them and consequences for such

organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

Home Country Regulations as Solutions

It is then possible to resolve these conflicts through adopting the principle that free speech and privacy are to be regulated only in the home country (the country of origin, to use the terminology of part) of the Internet use who publishes information or controls personal data.

The European Union data protection regime is specifically based on home country regulation, as the text of Art. 25 demonstrate. All the countries which implement the Directive have, by definition, an 'adequate' level of privacy protection, and the privacy of the data subject in respect of the transferred data is then a matter for the law of the controller's jurisdiction. The same applies to non-EEA countries to which data transfer is permitted under Art. 25 on the basis that an adequate level of protection is provided and the Directive contains provisions under which the European Commission can declare that particular countries provide adequate protection.[17]

[17] Directive 95/46/EC, Art 25 (6).

The same is true of other data protection laws,[18] provided there is international consensus on the basic principles under which privacy is to be protected, a home country system of regulation is workable.

The reason the answer 'yes' is qualified is because there are political and philosophical objections in some countries to establish state agencies to regulate privacy. However, the experience of the US Safe Harbor scheme suggests that workable solutions are likely to be found.

Home country regulation is far less likely to provide a workable mechanism for reconciling the conflicts between national laws which impose restrictions on free speech because there are wide variations in the restrictions which different countries deem appropriate. It seems unlikely that, in the medium term future at least, an international consensus on the minimum levels of free speech restriction will emerge,[19] and

[18] See e.g. Australian Privacy Act 1988; Canadian Privacy Act 1983, Personal Information Protection and Electronic Documents Bill (Bill C-6 of 1999); Hong Kong Personal Data (Privacy) Ordinance 1996.

[19] For a contrary argument, See Viktor Mayer-Schonberger and Tree E Easter Free Speech and the Global Information Infrastructure (1996-97) 56 Michigan Telecommunications and Technology Law Review 3 (45) at 45, 56-60, arguing that such a consensus can be built on the basis of the International law principle of Jus Cogens, defined in the Vienna Convention on the Law of Treaties (1969), Art 53 as a norm accepted and recognized by the international community of States as a whole as norm from which no derogation is permitted and which can be

without such a consensus home country regulation is impossible.

This, of course, will not prevent Internet users from publishing information, which contravenes the laws of foreign countries. The organizations will not be deterred from operating websites which are hosted on US servers merely because they are committing offences under French and German law, as it is not possible in practice for the national authorities to take effective action against foreign website operators. The danger, as the discussion at part illustrates, is that action taken against ISPs might lead to excessive self censorship of their systems. However, the emerging trend towards granting immunities to intermediaries will mitigate this risk. It may well be that the differences in national free speech laws are justified and should be maintained.

Privacy Policies & Website Compliance

To ensure compliance with data protection requirements when doing online transactions, it is mandatory to incorporate a

---

modified only by a subsequent norm of general International law having the same character.
However, it is apparent from their analysis that such a consensus would impose few restrictions on free speech, and would be far closer to the US First Amendment model than e.g. The German or the Saudi Arabian model. In the authors' view, it will be many years before there is sufficient cultural convergence to produce a Jus Cogens consensus, if indeed it ever happens.

privacy policy. A privacy policy is a statement of practices that the organization or corporation has to follow with regard to data collected and processed online, and can be very useful in increasing transparency for users and in complying with legal requirements.

Most web users want to understand that personal information they share will not be shared with anyone else without their permission. An annuals survey conducted by the Graphics, visualization and Usability Center of the Georgia Institute of Technology showed that 70% of the web users surveyed cited concerns about privacy as the main reason for not registering information with websites. 86% indicated that they wanted to be able to control their personal information. A study by TRUSTs revealed that 78% of users surveyed would be more likely to provide information to sites that offered privacy assurance.[20]

Privacy policy is an assurance by an entity about how they will deal with the data of individuals that they collect as part of their business. Privacy policies on the Internet are getting importance due to consciousness among people for the fear of losing privacy online. Privacy policies are basically a step

[20] See, http: //searchsecurity.techtarget.com.html

forward for self regulation and needs to be adopted by a website since people are ready to do e-commerce and are ready to divulge their details only on being assured about the privacy of their personal data. It induces confidence in people, and goes to the benefit of e-consumers and e-businesses. Keeping these things in view, an increasing number of websites have begun to provide privacy policies that detail the site information practices.

The information collection done by a website is generally e-mail address, name, phone number, postal address, age, gender, occupation, credit card number etc. In a policy, a website has to post clear details of what information they collect and how they use it, with whom they share it and whether any other companies are collecting information through their site.

The *world wide web* consortium's platform for *personal privacy project (P3P)* offers specific recommendation for practices that will let users define and share personal information with web sites that they agree to share with it. The P3P incorporates a number of industry proposals, including the open profiling standard (ops).

Using software that adheres to the P3P recommendations, users will be able to create a personal profile, all or parts of

which can be made accessible to a website as the user directs. A tool that will help a user decide whether to trust a given web site with personal information is a statement of privacy policy that a web site can post. In America, there is an organization called TRUSTe[21], which is an independent non profit internet privacy organization and which has been sponsored by giant corporations like AOL and Microsoft. It has a membership of about 600 companies, which are doing e-commerce worldwide. It monitors with websites of members to see whether their date collection techniques or their method are in conformity with privacy policies recognized worldwide and if that is so, they give a type of electronic seal to the company that is doing e-commerce.

The seal cannot be duplicated and they have measurer in place to see that any unauthorized person can not misuse it. So, any website having the seal means that the privacy policy of that company is in conformity and users will feel safe to divulge their details and can give their credit card numbers etc. there is also a complaint mechanism under this TRUSTe organization together with a dispute resolution mechanism, which is done online. In case a consumer is not satisfied with the privacy

[21] The use of TRUSTe may be seen on www.hotmail.com, which quite obviously deals with huge amounts of personal information.

policy or he is suspicious of a company with which he is dealing, he can complain to the organization. Several similar privacy programmes have been developed or are under developing stage of which BBB online and CPA web Trust are two important ones.

The cyberspace comes within the inherent dangers to privacy. Though the concept of privacy protection is old, creative interpretation of law is required to deal with new tools for tracking and stalking people on the information superhighway.

Human beings treasure privacy and link it to personal freedom, self-determination and well being and so have a right to control data about them. This is evident even when we roll back to the pages of history but consciousness for privacy got momentum, around the world, after the world-war II. During 1970's and 1980s data protection and privacy laws became much debated political issues and legislation on privacy was adopted in several European countries.[22]

At the same time, several big business establishments expressed their concern that these laws would extensively prevent the international flow of data. But in this world of rapid

[22] http:europa.eu.int/comm.

technological convergence such concern are difficult to sustain. In the 21st century e-organizations need to implement comprehensive privacy risk management programs to shield them from exposure as they move on towards their operations worldwide.

Using benchmarking tools, proven methodologies and diagnostics a business enterprise must detect and help to mitigate privacy risks and vulnerabilities.

To achieve this, strategies should include a comprehensive compliance process management of internal privacy employee training and awareness self-regulatory efforts, corporate interface with privacy awareness organization litigation support and alternative dispute resolution system.

Therefore, it is submitted that every e-organization's privacy practices should be benchmarked against national and international standards for privacy protection, fair and transparent information practices to be adopted to meet the emerging challenges globally.

Conclusion & Suggestions

Conclusion and Suggestions

Modern technological developments and in particular the so called convergence of computer and information communication technologies have created an environment in which there is ready access to personal information. It is critical not only for the protection of individual privacy but also a threat for information privacy i.e. data privacy. Accordingly, it is of vital importance to develop a comprehensive policy that may be able to create an enabling framework for overall protection of privacy and finding appropriate balance between privacy and other competing interests.

Therefore, a developing nation like India has to strive to maintain a balance between the provisions of universally applied laws and Indian legal infrastructure relating to convergence of technology mainly based upon information technology applications i.e. Telegraph, Electronic- media, Cable Broadcasting, Satellite and Internet.

Access to new technology (i.e. *Technology Inclusion*) is of utmost importance for the achievement of desired social and economic goals. Availability of affordable and effective communication medium for the citizens with due vision of care

for Information Privacy and security is also required with the evolution of international communication environment.

The formulation of possible corrective and co-operative actions in terms of control and regulation is the need of globally challenged environment of computers and Internet in a transparent manner.

Contemporary and radical developments in science and technology have shown serious impact on breach of confidentiality and privacy. The fusion of technology which is termed as convergence of computer and telecommunications technologies have created an environment in which there is very easy access to an ever growing storage and flow of personal information.

With the advent of the Internet, it has now become very easy to extract, exploit and to compile private and confidential information of individuals as well as state parties also. What were scattered, unimportant, small bits of data has now become a potent large set of data that can be captured and misused by unauthorized persons and anti-social elements. Considering these phenomenal developments many countries have enacted and adopted the legislations on control and regulation of privacy.

Privacy has no specific boundaries and it has different meanings for different people. It is the ability of an individual or group to control the flow of personal information regarding them and to keep their lives and personal matters out of public domain.

Immense concerns are already prevailing with respect to the protection of personal data and information, particularly relating to the right of one's privacy.

In India, as such, no specific privacy legislations has found place in legal framework as yet. In fact, the decisions of the Supreme Court of India on dynamic interpretation and construction of Article 21 are still the guiding principles.

The Constitution of India does not explicitly grant the fundamental right to privacy. However, the courts have read the right to privacy in relation to other existing Fundamental Rights such as Freedom of Speech and Expression under Article 19(1) (a) and 'Right to Life and Personal Liberty' under Article 21 as an extended horizon.

In India, the right to privacy is one of the un-enumerated rights so far granted to the individuals. It is also to note that the constitutional guarantee of the right to privacy is valid only

against the state and no constitutional remedy for violation of privacy lies against any individual explicitly. In addition, the violation of an individual's privacy per se is still not viewed as an offence in strict sense, only some remedy may be under Tort law or under the Indian Penal Code.

The existing standards and precedents with case to case development are the only solution to the problem. The courts in India have not yet had the opportunity to look at privacy issues on Internet. Analogies to the Internet will, therefore, have to be drawn from instances and cases that the court has actually dealt with.

At the same time, it may be presumed that the existing international standards and case precedents of the developed nations will have a significant impact on the Indian legal position and the decisions of the courts in India.

From a detailed and critical study of the legislative infrastructure with reference to right to privacy in India, it may fairly be stated that right to privacy is necessarily subservient to the national interests and national security at all times. However, in a democratic set up where personal liberties of individuals are recognized and protected, formulation of

appropriate legislative policy is the specific need in the current electronic environment.

The distinction between applicability and enforceability is fundamental to the future development of Internet law. It is a comparably easy task to make a law which applies to a particular activity undertaken via Information Technology but much more difficult to make the law so that it is enforceable in practice.

Laws which are unenforceable have some major defects i.e. not only do they fail to deal with the mischief which the law seeks to remedy, but the knowledge that they are unenforceable, weaken the normative force behind the law, thus, the law is complied with because of its normative force[1] i.e. because it is law.

The Information Technology related legislations have the problem of unenforceability due to the trans-jurisdictional nature of Internet activities. The system of law and regulations which needs to be enforceable is not simply that of a single jurisdiction, but that of all the jurisdictions whose laws are applicable to the whole range of activities.

---

[1] Kelsen; The Pure Theory of Law, University of California Press, Berkeley,(2nd Ed.) 1967, P.35

The growth of the Internet with the feature of 'always-on' connectivity for larger segments of population poses a very significant and new kind of security threats to individuals, society and states as a whole, as well as challenges to law enforcement agencies also. A law which is either unenforceable, or unenforced, falls into disrepute and loses its normative effect as law.[2] Law restricting free speech etc. is likely to be unenforceable against the persons outside the jurisdiction who use the Internet to disseminate information and services to persons outside. Freedom of communications, irrespective of the moral content communicated, is such a fundamental consequence of the information technology that even convergence of national laws seems unlikely to curtail that freedom to any extent. Ultimately restrictions of this kind, no matter how strong the argument in their favour, may be driven out of national law and replaced by filtering technology which, set to user's preferences, prevents the receipt of communication on unwanted topics. Thus, Internet as well as the related information technology as a whole has become a prominent social problem that makes it societal concern.

[2] Fuller; The Morality of Law , New Haven: Yale University Press 1964, Ch-II

The rights and interests of Internet users cannot be well protected by the existing laws and regulations. It is required to establish a comprehensive legal system on the protection of privacy, especially the privacy in cyberspace.

It is noteworthy that there are various ways of network infringement and the relevant application of the law under the existing laws and regulations on protection of privacy should be developed and enforced as global code namely 'Universal Internet Regulation Code'.

Keeping in mind the growth and implications of the information technology, especially the influence of the Internet and threat of privacy as an obstacle towards facilitating a secure environment for communication over the Internet, it is highly imperative to establish laws strictly pertaining to protection of privacy and personal data. It is equally important to note that the protection of personally identifiable information is vital if one seeks to foster a secured and protected electronic environment. Therefore, a legal framework needs to be established setting specific standards relating to the methods and purpose of assimilation of personal information and data over the cyberspace.

In this context, the role and corresponding duty of each country is to ensure the protection of privacy and to set relevant standards in a way to serve the needs and to harmonize national as well as international privacy and data protection legislations.

The 'right to privacy' as a right we all expect protection, we do not expect personal details such as our age, medical records, personal and family details, political and religious beliefs to be freely available to everybody. The ease of digitization of data and sharing it across networks means that personal information may not be so private anymore, which poses unforeseen risks.

With the growth of Information Communication Technology (ICT), large data bases are able to hold huge quantities of information and global networks are able to share and distribute this information around the world in no time. In order to control this and to protect the right to privacy the Data Protection Law is required. For this, reference can be taken from the Data Protection Act, 1998 in U. K. and Directive's of European Union on the protection of personal data in this regard.

Suggestions

In relation to privacy and Information Technology, privacy protection is very critical regarding the user's trust in the electronic environment and it is a necessary condition for the effective development of e-commerce and comprehensive system of e-governance. In practice, international community has accepted the right to privacy and data protection as a basic human right, therefore, in this scenario India may develop privacy and data protection legislations based on the moral and legal obligations.

It has been said that privacy is important because it is the basis on which we form meaningful relations with other people by deciding how much of ourselves to reveal or conceal to any given person and also a means of securing the trust which people expect in return for providing accurate information about themselves, a necessary condition for living in a society which values freedom and diversity.

It is important that legislators should be informed that the protection of personally identifiable information is vital if one seeks to poster a secure and trustworthy electronic transaction based on information Technology.

Considering the impact, the following suggestions are advanced to strengthen the legal infrastructure relating to Information Technology and its impact on several dimensions of privacy:

(1) The Indian Constitution does not guarantee the Right to Privacy as a fundamental right. The sole credit goes to the Indian judiciary for recognizing the concept of privacy because neither the Constitution nor any other statute has defined the concept. Still a lot more has to be done for the recognition and protection of privacy by law in India. As a matter of fact this concept is in primitive stage of its development but its development is bound to have tremendous effect on the individual's living with the development of Information Technology. Therefore, it is suggested that the 'Right to Privacy' should be recognized as a separate Fundamental Right with comprehensive guidelines on this sensitive issue of the privacy.

(2) The fundamental right of freedom of speech and expression as enshrined in the Constitution of India extends to the medium of Information Communication Technology as well and therefore every citizen has a freedom to acquire or share knowledge (or information)

using Information Technology and related sources, subject only to reasonable restrictions. Since, imposing "reasonable restrictions" on the Information Communication Technology has certain limitations; therefore a legal framework based on the principle of 'reasonableness and due care' has to be adopted. For this purpose, the Information Technology Act, 2000 may be amended and enlarged to equate it with the concept of "balanced flow of information".

(3) The right of an individual to protect his personal information is a basic civil right, and is recognized as such the world over. Thus in relation to data and individual privacy, India should enact legislation to protect the personal data of individuals, and to ensure that data collected for a particular purpose is used for that specific purpose only.

(4) Governments and other empowered authorities are interested in what passes over on the Internet and are making efforts to devise various means of exercising a substantive degree of control by way of interception in relation to information communication technologies, as a consequence the organizations and individuals using these

techniques are concerned with their privacy and security of data. These genuine concerns can be meted out by wide application of encryption methods to control the privacy of data and theft of valuable information.

(5) Earlier, before the enactment of Information Technology Act, 2000, no legal infrastructure was available in Indian legal context, which explicitly recognized or denied the general principle that information, records in electronic form should be given legal effect.

Since, the Information Technology Act, 2000, intended to deal with computer abuse and e-commerce matters, contains brief mentions of data protection issues but does not lay down specific privacy principles.

Yet the making of Information Technology Act, 2000 was a landmark in Indian legislative history to combat with emerging and developing technological threats, but in this era of diagonal changes in technology the frictional changes in law is also required to resolve the maladies.

(6) The present Information Technology (IT) Act is soft when it comes to curb cyber criminality, thus there is need for

more deterrence in the IT Act. Cyber crimes have to be dealt with very strongly because this is being done by knowledgeable people and to deal with it the need of the hour is for training the investigating, prosecuting and judicial agencies to respond to the challenges posed by cyber criminals.

(7) The technical advancements and convergence of Internet and telecommunication technologies precludes a central control, which may be controlled and regulated by concerned empowered authorities and governments by adopting new and effective means of cyber security.

(8) The fact that so many records and information is maintained in electronic format, or is more readily usable in electronic form, therefore, the distinction between manual records and electronic records must be minimized to give effect the digital form of records in relation to promote e-transactions in present times.

(9) The balance must be struck in relation to the extent of legislative provisions and variations by agreement in regular format of paper based transactions, that flexibility should be maintained in information technology based transactions i.e. electronic transactions. This should be

subject to fairness and reasonableness test as applicable in common legal parlance.

(10) The law in India includes a number of different provisions, which requires a documentation to be in writing. In a number of cases, it is unlikely that an electronic form of document would satisfy these requirements. It is imperative that a data message should satisfy any of these requirements for information to be in writing. This may be developed on functional equivalence to the United Nations Commission on International Trade Law (*'UNCITRAL'*) working group on Electronic Commerce completed work on its model law on Electronic Commerce in 1996, and its draft on international legislation on information security.

(11) The controlling and regulating authorities have the immense duty to evolve, develop and to up-date the rules and practices which recognize the new computer based technology for the effective implementation of e-governance and at the same time to protect the national as well as public interest.

(12) An information infrastructure already exists, but it is not integrated as a whole. Telephones, radio, transistors,

televisions, computers and fax machines are used everyday to receive, store, process, perform, display and to transmit data, text, voice, sound and images in offices, homes as well as in business within the country and outside the country. The above mentioned separate communication networks required an integration of legal control and regulation framework as digital code.

(13) The Indian communication system is still governed by more than hundred years old law legislations mainly the Indian Telegraph Act, 1885 and supported by the Indian Wireless Act, 1933. Considering the substantial technological developments and changes these laws must be replaced by new legislations giving effect to emerging scenario of digital technology.

(14) Convergence of technologies is very much in vogue in the area of broadcasting, information and communication sector, thus, there is urgent need of new legal framework to regulate the current developments in conformity with international standards.

(15) With the advent of new technologies such as GIS (Geographic Information Systems), and GPS (Global Positioning System) technologies used from space based

platforms, these surveillance techniques raises concerns about privacy rights, public safety and national security as well. Thus it is very necessary to develop and to incorporate the legal doctrines that may help to control these and related aspects of cyberspace surveillance.

(16) As per agency to regulate telecom sector i.e. 'Telecom Regulatory Authority of India' (TRAI) was established in 1997, the regulator for cyberspace may also be made possible with proposed name as 'Cyber Regulatory Authority of India' (CRAI), to control and regulate the activities on cyberspace.

(17) In the present Indian scenario the efficiency and effectiveness in the implementation of cyber regulations and control measures require structural changes in the framework as well as strengthening the e-court infrastructure and their capabilities to deliver the speedy justice. The public education regarding the use of cyberspace is immensely needed to educate and aware the general public in relation to cyber based criminality and related developments.

In view of inherent technical difficulties and radical changes in application of technology, it is high time to rethink

cyber laws to provide protection to users by developing the techno-legal framework in order to optimize more creative side or benefits of information communication technologies.

In short, every one should be aware of and actively involve in preventing and solving together the destructive side of information communication technology with an appropriate balance between regulations and self regulations subject to the different types of activities in cyberspace.

To keep up with the pace of technological innovations laws should be rethought with the impact of Internet in mind to ensure the integrity of cherished human values of privacy.

Last but not the least, the law must be synchronized and developed with all possibilities to sustain the good moral and ethical values in order to overcome the challenges posed by technological advancements. The uniformity in law and universal codification of Internet law must be evolved by the world community to protect the privacy and confidentiality in this database driven age.

Selected Bibliography

SELECTED BIBLIOGRAPHY

PRIMARY SOURCES

Act and Statutes

- The Information Technology Act, 2000
- The Constitution of India
- The Indian Telegraph Act, 1885
- The India Penal Code, 1860
- The Indian Wireless Act, 1933
- The Freedom of Information Act, 2002
- The Right to Information Act, 2005
- THE TRAI , 1997
- The Indian Evidence Act, 1872
- The Telegraph Wires (Unlawful Possession) Act, 1950
- The U.K Data Protection Act, 1998
- The U.K. Telecommunications Act, 1994
- The U.K. Electronic Communications Act, 2000
- The E.U. Data protection Act, 1998

- The U.S Economic Espionage Act, 1996
- The U.S Electronic Funds Transfer Act, 1978
- The U.S Uniform Computer Information Transactions Act, 1999
- The U.S Privacy Act, 1974
- The U.S Electronic Communications Privacy Act, 1986
- The U.S. Patriot Act, 2001
- The U.S. Child Online Protection Act, 1998
- The U.S Gramm-Leach-Bliley Act, 1999
- The U.S Health Insurance Portability and Accountability Act (HIPAA), 1996
- The U.S Computer Fund and Abuse Act, 1984

Conventions

- UNCITRAL Model Law on Electronic Commerce 1996
- UNCITRAL Model Law on Electronic Signatures 2001
- United Nations Declarations on Human Rights 1948
- European Convention on Human Rights and Fundamental Freedoms 1950

- Council of Europe Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Strasbourg 1981

Directives (European Communities Legislations)

- DIRECTIVE 95/46 (Legal Protection of Personal Data)
- DIRECTIVE 96/9 (Legal Protection of Databases)
- DIRECTIVE 97/66 (Telecommunications Privacy Directive)

SECONDARY SOURCES

Books

Akshay Kumar : Information Technology - An Info Guide AuthorsPress, New Delhi, 2000

Basu, D.D. : Shorter Constitution of India,13th Edn., Wadhwa, Nagpur,2001

Camacha , Teresa Fuentes : The International Dimension of Cyberspace Law, Vol. I, Ashgate Pub. Ltd., England , 2000

Cavazos A. Edward and Morin Gavino : Cyberspace and the Law, MIT Press, New York,1995

Cherles P. Pfleeger, Shari Lawrence Pfleager Security in Computing : (3rd Edn.) Pub,By- Pearson / prentice hall (Pearson Education, Inc.) (Indian Branch) Delhi, (6thIndian Reprint, 2005)

Choubey,R.K. : An Introduction to Cyber Crime and Cyber Law, 2007

Chris Reed & John Angel (Eds.) : Computer Law , 4th Edn. Universal Law Pub., Delhi, (Indian Reprint 2002)

Chris Reed : Internet Law ,Text and Materials, Second Edition, Universal law Pub Co. Ltd, Delhi (2005)

D.P.Mitttal: Law of Information Technology (Cyber Law), 2000

Deepti Chopra and Keith Merril : Cyber Criminals and Internet, I.K. International Ltd., New Delhi, 2002

Devnoy Chris : 'The Unwired Nation' ,Windows Sources (1994)

Diwan, Parag and Shamni Kapoor : Cyber & E-commerce Laws, Bharat Publishing House, New Delhi, 2000

Dr.R.K.Tiwari, P.K.Shastry and K.V.Ravikumar : Computer Crime and Computer Forensic, Select Publishers,Delhi,2002

Edwards , Lillian & Charlotte waelde, (Eds.) : Law and the Internet: Regulating Cyber Space Mart publishing : Ox ford 1997

Fadia Ankit : The Ethical Hacking Guide to Corporate Security, Macmillan India Ltd., First Pub. 2004.

Ferrera, G.R.,Lichtenstein, D.S.Reder,M.E.K., August, R., Schiano, W.T. : Cyber Law-Text and Cases,West Thomson Learning,USA,2000

Gringras Clive : The Laws of The Internet , Butterworths: London 1997

Innovation in Information Systems and Technology (Advanced Research Series): Macmillan Pub. India Ltd., First Pub., 2009

International Year Book of Law, Computers and Technology (2007)

James Michael : Privacy and Human Rights (UNESCO 1994)

Margrate Jane Radin, John A. Rothchild, Gregory M.Silverman: Internet Commerce: The Emerging Legal Framework, University Casebook Series, Foundation Press, 2002

Nandan Kamath (Ed.) : Law Relating to Computers Internet & E- Commerce, Universal Law Pub.Co.Ltd., Delhi., (Reprint 2005)

Pandey, J.N. : Constitutional Law of India, 34th Edn., Central Law Agency,Allahabad,1999

Peter Norton : Introduction to Computers, Tata McGraw-Hill, New Delhi, 1998

R.K.Suri,Parag Diwan,Shammi Kapoor (Eds.): Information Technology Laws, Pentagon Press, Delhi

Rahul Matthan: The Law Relating to Computer and the Internet, (2000)

Ranbir Singh and Ghanshyam Singh (Eds.) : Cyber Space and The Law –Issues and Challenges, NAL SAR University, Hyderabad Publications, First Published 2004

Ratan Lal & Dheeraj Lal : The Indian Penal Code,28th Edn., Wadhwa, Nagpur,2002

Rodney D. Ryder : Guide to Cyber Laws 1st Ed. 2001

S.M.A. QADRI (Ed.): Ahmad Siddique's Criminology & Penology, 6th Edn., Eastern Book Co., Lucknow, 2009

S.V. Jogarao : Law Relating to Information VOL-I & II. (2007)

Seervai,H.M. : Constitutional Law of India,2nd Edn. Universal Law Pub. Co.Ltd., 1975

Shahi, M.P. : Crime and Corruption in the Digital Age, 1st Edn., Authors Press,Delhi,2000

Shakil Ahmed Syed and Rajiv Raheja : A Guide to Information Technology (Cyber Law and E-Commerce), 2001

Sharma Vakul : Information Technology –Law & Practice Cyber Law & E-Commerce, Universal Pub. Ltd., Delhi, Reprint 2005

Sharma, Vakul : Handbook of Cyber Laws, Macmillan, India, 2002

Stallings William : Cryptography and Network Security, Prentice- Hall, 1999

Suresh T. Vishwanathan : The Indian Cyber Law, 2nd Edn., 2000

T.V.R. Satya Prasad : Law Relating to Information Technology (Cyber Law),1st Ed., 2001

Tanenbaum, Andrew S. : Computers Networks, Prentice Hall, 1996

Taylor,Paul A. : Hackers: Crime in the Digital Sublime, Routledge, London 1999

Upadhyay,J.J.R. : Administrative Law,2nd Edn., Central Law Agency, Allahabad,1997

V.N. Shukla's : Constitution of India, 9th Edn., Eastern Book Co., Lucknow, 2001

Verma S. K.,(Ed.) : Legal Dimensions of Cyber Space, Indian Law Institute, New Delhi (2004)

Verma, S.K. & Kusum (Eds.) : Fifty Years of the Supreme Court of India: Its Grasp and Reach, Indian Law Institute, Oxford University Press,2000

Wall, David S. (Ed.) : Crime and the Internet, Routledge, London, 2001

Westin, A.F. : Privacy and Freedom, Bodely Head, 1967

ARTICLES

Madhavi Divan, "The Right to Privacy in the Age of Information and Communications", (2002) 4 SCC (Jour) 12

Devashish Bharuka , "Piercing the Privacy Veil: A Renewed Threat", (2003) 1 SCC (Jour) 23

Subhashini Narasimhan and Thriyambak J. Kannan, "Right of publicity: Is It Encompassed in the Right of Privacy?", (2005) 5 SCC (Jour) 5

Thriyambak J. Kannan and Subhashini Narasimhan , "The Right to Privacy of Public Persons", 4 JSLC (2004) 74

Abhinav Chandrachud, "The Substantive Right to Privacy: Tracing the Doctrinal Shadowes of the Indian Constitution", (2006) 3 SCC (I) 31

B.D. Agarwala, "Right to Privacy: A Case- By- case Development" , (1996)3 SCC) (Jour) 9

Faizan Mustafa, "Privacy Issues in data protection National and International laws", (2004) PL Web Jour 16

Shashank Manish, "Regulation of Cyber Crime in India", Cri L J – Nov 2008 - Journal Section , PP.305-312

Kartikey Mahajan & Kanishk Kakkar," Cyber Trespass – Plugging the Loop Holes in the Law",

Cri L J- Nov 2008 - Journal section, PP.321-328

Gurjeet Singh and Vicky Sandhu, "Emergence of Cyber Crime: A Challenge for the New Millennium", Delhi Law Review, Delhi, PP.25-57

Dhruv Jain,"The Right to Privacy in India: An Overview" , AIR -June 2009 VOL. 96 Journal Section, PP. 90-96

Samuel Warren and Louis Brandis, "The Right to Privacy", Harward Law Review 4, 1890, PP.193-220

Pavan Duggal , "Cyber Law- An Overview", available at http://www.cyberlawindia.com

Pavan Duggal , "Cyberlaw 2001:Two Dramatic Developments", available at http://www.zdnet.com

Nayan Ranjan Sinha and Ravi Shekhar Vishal, "The Indian Cyber Law and Legal Issues", First Pub. 2009 (Advanced Research Series), Innovation in Information Systems and Technology, MacMillan Pub. India Ltd., PP.153-161

Atul Bamrara, "Cyber Crimes In the Era of Globlisation", Gumbad Business Review, Vol.3, No. 1(2007), PP.69-77

Journals

- All India Reporter (AIR)
- Criminal Law Journal (Cri. L J)
- Journal of Information, Law and Technology (JILT)
- Supreme Court Cases (SCC)
- SCC Online
- Journal of Indian Law Institute

Magazine

- Lawz.
- Practical Lawyer
- Lawyers Update
- Frontline
- Computer Today

News Papers

- The Hindu, New Delhi
- The Times of India, New Delhi
- The Hindustan Times, Delhi.

Websites

- www.cca.gov.sg/eta
- www.cli.org
- www.cyberlawindia.com
- www.cyberspacelaws.com
- www.crypto.org
- www.ecommerce.gov
- www.findlaw.com
- www.giic.org
- www.mit.gov.in
- www.supremecourtonline.com
- www.uncitral.org
- www.wto.org

GLOSSARY OF TERMS

ARPANET A network begun a an experiment by the U.S government in packet switched technology, that linked a largely technical audience of the military, government agencies and academic researchers and scientists and formed the basis of the Internet.

Artificial intelligence (AI) The study of thought processes of humans and representation of those processes via machines (computer, robots and so on).

Artificial neural networks (ANN) The technology that attempts to achieve knowledge representation and processing large amounts of information and the ability to recognize patterns based on experiences.

Asynchronous transfer mode (ATM) Data transmission technology that divides data into uniform cells, creates a virtual connection for the packet transmission and eliminates the need for protocol conversion.

Automatic number identification (ANI) Service in which the number of an incoming call is identified and displayed to the person receiving the call also known as *caller ID*

Backup An extra copy of data and programs kept in a secured location (s).

Bandwidth The range of frequencies available in a communications channel sated in bits per second the greater the bandwidth the greater the channel capacity.

Biometric controls Automated methods of verifying the identity of a person based on unique physiological or behavioral characteristics such as finger or retina prints voice, or keystroke dynamics.

Bit Short for binary digit (0s and 1s), the data the CPUs can process.

Blue tooth A wireless technology that allows digital devices to communicate with each other via low- power radio frequencies.

Broadband Communication channel bandwidth with the highest capacity, used by microwave cable and fiber-optic lines.

Browsers Software application through which users access the Web; these application communicate via HTTP, manage HTML and display certain data types for graphics and sound.

Byte An 8-bit string of data, needed to represent any one alphanumeric character of simple mathematical operation.

Cache memory A type of primary storage, close to the CPU than is RAM, where the compute can temporarily store blocks of data used more often.

Cathode ray tube (CRT) Technology, used in most monitors in witch beams of electrons illuminate pixels on a computer screen.

Central processing unit (CPU) The part of the computer that performs the computation or "number crunching"; also called microprocessor.

Centralized database Database with all of the related data files stored in one location.

Clickstream data Data that can be collected automatically from a company's Web site.

Clipping service Service that tracks and retrieves artieves articles on particular topies from electronic datanbases.

Code of ethics A collection of principle intended as a guide of members of company of an organization.

Compute network Communications media, devices and based softwere needed to connect two or more computer systems and/ or devices.

Compute programs Sequences of instructions for the computer.

Cookie A small data file placed on users' hard drives when they first visit a site that can exchange information automatically between a server and a browser and can be used to track users' actions and preferences.

Cracker A malicious hacker who may represent a serious problem for an organization.

Cross-border data transfer The flow of corporate data across national borders; laws regulating such transfer are inconsistent from country to country, though efforts at standardization are underway.

Customized catalog Catalog assembled specifically for a particular company, usually customer of the a particular company usually a regular customer of the catalog ower.

Data Raw facts or elementary descriptions of things, events, activities and transactions that are captured, recorded, stored and classified but not organized to convey any specific meaning.

Data definition language (DDL) Description of each data element in a database and the relationship among the records.

Data management The storage, retrieval and manipulation of related data.

Data manipulation language (DML) Instructions used with higher-level programming languages to query the contents of a database, store or update information therein and develop database applications.

Data mining A process of looking for unknown relationship an and patterns and extracting useful information from volumes of data using tools such as neural computing of case based reasoning.

Data quality (DQ) A measure of accuracy, completeness, timeliness, consistency, accessibility security or other characteristics that describe useful data.

Database A logical grouping of related files.

Database management system (DBMS) The software program of group of program that provide access to a database.

Decryption Transformation of scrambled code into readable data after transmission.

Desktop personal computer The typical microcomputer system used as a standard tool in business and the home.

Digital certificates Electronic identification cards that give access to an intranet.

Digital signature Authorising signature added to electronic messages or electronic checks, usually in encrypted format.

Domain name The official name assigned to an Internet site consisting of multiple parts separated by dots which are translated from right to left in locating the site.

Dynamic data Data that continuously change.

Dynamic HTML A next step beyond HTML which lets users interact with the content of richly formatted pages without having to download additional content from the server.

E-business A broad definition of electronic commerce that refers not just to buying and selling but also to servicing customers collaborating with business partners and conducting electronic transactions within an organization.

Electronic banking Various banking activities from paying bills to securing loans conducted over the Internet or private

networks (Also called *cyberbanking, virtual banking, home banking and online banking)*

Electronic certificate Verification provided by a trusted third party (a certificate authority) that a specific public key belogs to a specific individual.

Electronic checks (e-checks) Payment mechanism similar to regular bank checks but transitted electronically with a signature in digital form rather than as paper checks.

Electronic commerce (EC) The buying and selling of products, services and information via computer networks primarily the Internet.

Electronic data interchange (EDI) Application that electronically transmits routine, repetitive business document directly between the computer system of separate companies doing business with each other.

Electronic funds transfer (EFT) Application that electronically routes funds debits and credits and charges and payments among bank and between bank and customers using telecommunication networks.

Electronic government (e-government) The use of Internet technology in general and electronic commerce in particular to deliver information and public services to citizens, business partners and suppliers and those working in the public sector.

Electronic mail (e-mail) Application than can electronically manipulate, store and transmit computer –based messages through telephone wires or wireless networks.

Electronic mall A collection of individual shops offering many products and service under one Internet address (Also called *cybermall and e-mall).*

Electronic surveillance The tracking of people's activities online or offline with the aid of computers.

Eneryption A process of marking messages or data indecipherable prior to their transmission to protect them from unwarranted access. Those who have an authorized decryption key which uses a code composed of a very large collection of letters, symbols and numbers are able to decipher it.

Ethernet The most common protocol used by more than three fourths of all networks.

Ethics The branch of philosophy that deals with what is considered to be right and wrong.

External data Data generated outside an organization.

Extranets Secure networks that link business partners and intranets over the Internet by providing access to areas of each other's corporate intranets extended intranets.

Facsimile (fax) Application that converts and sends the white and black as of a page over telephone wires or wireless networks to a receiving machine that converts the coding back in to white and black areas and prints the massage.

File A logical grouping of related records.

File transfer protocol (FTP) Protocol that enables users to access a remote computer and retrieve files from it.

Firewall A security device located between a firm's intranet and external network (e.g. the Internet)regulates access into and out of a company's network commonly a barrier between a secure internal network and the Internet which is assumed to be unsecured.

Flash memory A form of read-only memory on a silicon computer chip that is compact , portable has limited capacity and requires little energy.

Geographical information system (GIS) A data visualization technology that captures, stores, checks , integrates, manipulates and displays data using digitized maps.

Gigabyte Approximately 1 billion bytes.

Global information system (GIS) Interorganizational in formation system that connect companies located in two or more countries. Companies connected by such systems may be multinational, international or virtual.

Global positioning system (GPS) A wireless system that uses satellites to enable users to determine their position anywhere on the earth.

Graphical user interface (GUI) System software that allows users to have direct control of visible objects such as icons and actions that replace command syntax.

Hacker Person outside an organization who penetrates its computer system.

Home page A text and graphical screen display that welcomes the user and explains the organization that has established the page; in most cases will lead used users to other pages.

Hypermedia The links that connect data nodes in hypertext.

Hypertext document The combination of nodes, links and supporting indexes for any particular topic.

Hypertext Markup Language (HTML) The standard programming language used to create and recognize documents on the world wide wave without changing the original information; incorporates dynamic hypertext links to other document stored on the same of different computers.

Hypertext Transfer Protocol (HTTP) The communication standard used to transfer pages across the Web; defines how messages are formatted and transmitted.

Information A collection of facts (data) organized in some way so that they are meaningful to a recipient.

Information system (IS) A system that collects, processes, stores and analyzed data and disseminates information for a specific purpose.

Information technology (IT) A particular component for a computer- based information system.

Infrared Red light not commonly visible to human eyes, modulated or pulsed for conveying information.

Integrated services digital network (ISDN) High-speed transmission technology that allows users to simultaneously transfer voice, video, image and other data at high speed.

Internal data Data generated by the corporate transaction processing system, functional user information system and other functions and individuals inside an organization.

Internet A massive electronic and telecommunications network connectiing the computer of businesses, consumers, government agencies, school and other organization worldwide , which exchanges information seamlessly using open , nonproprietary standards and protocols.

Internet fax Facsimile transmission of documents from a desktop computer on the sender's end to a standard fax machine on the receiver's end through a fax server in an ISP's network.

Internet service provider (ISP) Company whose primary business is to provide its customer with connections to the internet.

Intranet telephony A service that lets users talk across the internet to any personal computer equipped to receive the call even around the world for the price of only the Internet connection.

Intranet A private network that uses Internet software and TCP/IP protocols in essence a private Internet or group of private segments of the public Internet network.

IP address An assigned address for each computer on the Internet that distinguished it from other computers consists of four sets of numbers separated by dots.

Knowledge database Data model that stores decision rules that can be used for expert decision making.

Laptop computer Transportable , lightweight microcomputer

Magnetic diskette A form of easily portable secondary storage on flexible Mylar disks; also called floppy disks.

Magnetic tape A from of secondary storage on large open reels or smaller cartridge or cassette.

Management information system (MIS) A system that accesses , organizes and reports on organizational information needed for repetitive decision making in functional areas, usually by middle managers.

Memory cards Credit card sized devices used as storage devices in personal computers.

Message Instruction from another object that activates operation contained within the object receiving the message.

Metadata Data about data.

Microcomputer (personal computer, PC) The smallest and least expensive category of general purpose computers.

Microphone Input device for voice-recognition software.

Microprocessor The CPU , make millions of microscopic transistors embedded in a circuit on a silicon wafer or "chip" ;commonly referred to as chips.

Mobile computing Transmission of data to and from mobile computers on radio-based networks.

Mobile Internet (wireless Web) The use of wireless communications technologies to access network-based information and application from mobile devices.

Modem Device that converts signals from analog to digital and vice versa; contraction of the terms *modulate and demodulate.*

Monitor The video screen used with most computers, which display both input and output.

Mouse Hand held device used to point a cursor at a desired place on a computer screen; a click instructs the computer to take some action.

Multimedia database Data model that can store data on many media.

Multimedia technology The computer- based integration of text, sound still images, animation and digitized motion video.

Network A connecting system that permits the sharing of resources among different computers.

Newsgroup Discussion group on the Internet in which an international audience is able to post on an electronic bulletin board ideas on various topics also called a forum.

Notebook computer Transportable, lightweight microcomputer that fits easily in to a briefcase.

Optical mark reader Optical scanner that reads pencil marks made on a predetermined grid.

Optical mouse A mouse where a light, lens and camera chip replace the ball , rollers , and wheels of the standard mechanical mouse ; the optical mouse takes pictures of the surface it passes over and compares successive images to determine where it is going.

Pages Application programs or modules of fixed length for use in virtual memory.

Palmtop computer Hand-Held microcomputer that is small enough carry in one hand.

Pen mouse A variant of the standard mouse , the pen mouse resembles and automobile stick in a gear box; moving the pen and pushing buttons on it move the cursor on the screen.

Pixels Tiny points on a computer screen that are illuminated by electrons.

Privacy policies Codes that state an organization's guidelines with respect to protecting the privacy of customers , clients and employees.

Private key One of two codes used in a public/private key encryption system the private key is know only to its owner but not to those who have the public key.

Programming The translation of the design specifications into computer code; typically a time-consuming and costly process.

Protocol The set of rules and procedures that govern transmission across a network, principally line access and collision avoidance.

Prototype Small- scale working model of a new larger computer system.

Public key security The Protection of intranet from outside intrusion and integration of them with the public network.

Public key One of two codes used in a public/ private key encryption system ; the public key is encrypting or decrypting messages.

Public key infrastructure (PKI) A security system based on use of two keys and also including a digital signature and a certificate.

Public/private key encryption Security encryption system that uses two different keys, one public and the other private one used for encryption and the other for decryption .

Random access memory (RAM) The part of primary storage that hold a software program (or a portion of it) and small amounts of data when they are brought from secondary storage.

Raw data Data that have not been processed.

Read-only memory (ROM) A type of primary storage where certain critical instructions are safeguarded because the storage is nonvolatile and the instruction can be read only by the computer and not changed by user.

Record A logical grouping of related fields.

Search engine Program that finds and lists Websites or pages (designated by URLs) that some user selected criteria.

Secure Electronic Transaction (SET) protocol More Comprehensive protocol for credit card processing that

incorporates digital signatures, certification, encryption and an agreed-upon payment gateway to banks.

Security The operating system's control of access to files held in secondary storage.

Sensor Input device embedded in various technologies that collects data directly from the environment and inputs them into a computer system.

Servers Smaller types of midrange computers that support computer networks, enabling users to there files, software peripheral devices and other network resources.

Single-key encryption The sender of the electronic message encrypts the information with a key, receiver uses an identical key to decrypt the information.

Smart cards Plastic cards, like credit cards that contain a microprocessor capable of storing and processing a considerable amount of information; can be used for electronic payments storing a computerized value of funds that is drawn down as used.

Software A set of computer programs that enables the hardware to process data.

Spamming Indiscriminate distribution of e-mail messages (junk e-mail)

Supercomputer Computer with the most processing power used in scientific and military work and increasingly in business for simulation, modeling and other types of computation intensive analysis.

Surfing The process of navigating around the Web by means of pointing and clicking a graphical Web browser.

Synchronous optical network (SONET) An interface standard for transporting digital over fiber-optic lines that allows the integration of transmissions from multiple vendors.

Telecommuting Generally refers to the ability of employees to work at home at a customer's premises, or while traveling by using a computer linked to their place of employment; also called *teleworking.*

Telematics system Services powered by wireless communications, global positioning systems and onboard electronics that provide location, navigation, traffic monitoring and control, toll collection and travel information.

Telnet Protocol that establishes an error-free link between the two computers and so allows users to be on one computer while doing work on another.

Terabyte Approximately 1 trillion bytes.

Text mining The application of data mining to non structured or less structured text files.

Topology The physical layout and connectivity of a network.

Touch screen Computer screen divided into different areas which the user touches to trigger an action.

Transmission Control Protocol/Internet (TCP/IP) A file transfer protocol that can send large files of information across sometimes unreliable networks; the protocol of the Internet.

Unified modeling language(UML) A language for specifying, visualizing, constructing and documenting the artifacts (such as classes, objects etc) in object-oriented software systems.

Uniform resource locator (URL) The set of letters that points because to the address of specific resource on the Web.

UNIX Operating system used by many business organization because it provides many sophisticated desktop features on many different sizes and types of computers.

USENET A protocol that gathers and stores e-mail messages categorized by topic and delineates how groups of messages can be stored on and sent between computers.

Videoconferencing Application that electronically enables two or more people to have face-to face communications with a group in another location without having to be present in person.

Virtual banks As opposed to regular banks with added online services, virtual banks are dedicated solely to Internet transactions.

Virtual memory A feature that simulates more main memory than actually exists in the computer system by extending primary storage into secondary storage.

Virtual private network (VPN) A wide area network operated by a common carrier provides; a gateway between a corporate LAN and the Internet.

Virus Software that can damage or destroy data or software by attaching itself to other compute programs.

Web crawler A search engine that traverses the Web automatically, collecting index data; variously called spiders, ants, robots, bots and agents.

Web site All the pages of a particular company or individual.

Wide area network (WAN) Network that cover wide geographic areas and include regional network such as telephone companies or international network such as global communication service providers; may be commercial, privately owned, or public.

World Wide Web A portion of the Internet that uses the transport functions of the Internet, via a client/server architecture, to handle all types of digital information, including text hypermedia, graphics and sound.

.....
.....
.....